enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

5G CYBERSECURITY STANDARDS

Analysis of standardisation requirements in support of cybersecurity policy

MARCH 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use erika.magonara@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

François Cosquer, François Zamora, Alf Zugenmaier

EDITORS

Erika Magonara, Sławomir Górniak – ENISA

ACKNOWLEDGEMENTS

ENISA would like to thank Ms. Elżbieta Andrukiewicz and Mr. Jordi Batalla for their support to the study, reviews and comments.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-568-5 DOI 10.2824/700472

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The ambition of this report is to outline the contribution of standardisation to the mitigation of technical risks, and therefore to trust and resilience, in the 5G ecosystem. The 5G ecosystem considered in this report is a multi-dimensional space encompassing not only technological and functional domains, but also the related technology lifecycle processes and stakeholders.

This report focuses on standardisation from a technical and organisational perspective. Considerations of the effectiveness of specific standards and of the strategic aspects related to 5G security, although important, are outside the scope of this report.

Accordingly, this report:

- **Collects** standards, specifications and guidelines[1] relevant to the cybersecurity of the 5G ecosystem that had been published, either as drafts or in their final versions, by September 2021;
- **Positions** them within the defined 5G ecosystem by assessing the extent to which they address security objectives;
- **Identifies gaps in standardisation** by comparing the existing literature against an ideal situation of cybersecurity robustness and resilience, where standardisation addresses the necessary technical and organisational security aspects;
- **Formulates recommendations** on standardisation in the area of 5G cybersecurity.

The report collects and analyses more than 140 documents and positions them across 150 security measures. The main observations that can be derived from the analysis are the following.

- All in all, available standards, specifications and guidelines are general. They can be applied consistently to the 5G technical and functional domains and related lifecycle processes only after being tailored accordingly.
- 5G-specific standards, specifications and guidelines are available to a greater extent to the stakeholders of the telecommunication sector than for other stakeholders (e.g. audit organisations and stakeholders in the connected devices industry).
- 5G-specific standards, specifications and guidelines cover to a greater extent the ‘run’ phase of a technology lifecycle, whereas other phases would need tailoring.
- Existing knowledge bases on cybersecurity threats and IT-security guidelines can be used for 5G cloud native architectures and architectures relying on APIs (Application Programming Interface). Although these families of software are well known to the IT industry, their use is quite recent and constitute drivers of the ‘cloudification’ of the telecom sector.
- The existing literature does not allow for ‘end-to-end’ trust and resilience in the 5G ecosystem. For example, guidelines for 5G-specific tools and key performance indicators could be needed to ensure a common understanding of 5G protection and of end-to-end trust and resilience.

Concerning gaps in standardisation, the report finds that only the areas of governance and risk management as well as the security of human resources present moderate gaps e.g. related to sector-specific risk management. The other areas considered (e.g. operations management,

[1] Section 2.2 explains the taxonomy used by the document. For convenience the report refers to all considered documents alternatively as ’standards, specifications, guidelines’, ‘existing literature’, ‘reference documents’.

business continuity management and incident management) present major gaps in standardisation.

Still, this report recommends the adoption of a progressive approach to 5G standardisation, which should consider several elements such as the usefulness and necessity of new standards and their link with strategic objectives. It also notes the importance of fostering the maturity and the completeness of the identification and assessment of risk by harmonising risk assessment practices in a way that is inclusive of all stakeholders in the 5G ecosystem.

Finally, this report stresses that, while the technical and organisational standards analysed can contribute to the security of 5G, they should not be treated as an exhaustive list of measures guaranteeing security. There are risks that are not covered by standards, for example residual risks whose cost is neither borne by nor attributable to a specific stakeholder, such as societal risks resulting from network malfunctions. Indeed, the complexity of 5G calls for a comprehensive vision of trust and of resilience that goes beyond standardisation. This vision should be future-proof and not dependent on the variability of assets and configurations in the network.

1. INTRODUCTION

1.1 DOCUMENT PURPOSE AND OBJECTIVES

The ambition of this document is to outline the contribution of standardisation to the mitigation of technical risks, and therefore to trust and resilience, in the 5G ecosystem. Accordingly, the objectives of the document are:

- to provide an overview of standards, specifications and guidelines[2] relevant to the cybersecurity of the 5G ecosystem and that had been published, either as drafts or in their final versions, by September 2021;
- to facilitate the positioning and to assess the applicability of any reference document in the 5G security environment;
- to formulate recommendations on standardisation in the area of 5G security.

The document focuses on standardisation from a technical and organisational perspective. Considerations of the effectiveness of specific standards and of the strategic and policy aspects related to 5G security, although important, are outside the scope of this report.

Note on the relation to other on-going work on 5G cybersecurity carried out by ENISA: this report is not intended to pre-conceive any work related to the drafting of the European cybersecurity certification candidate scheme on 5G networks.

1.2 OVERVIEW AND STRUCTURE OF THE STUDY

Businesses and institutions participate in several activities concerning 5G networks and 5G-dependent processes: their design, construction, operation, introduction to the market, use, audit and even certification. Altogether, with various degrees of importance, they contribute to the Digital Single Market.

The EU Cybersecurity Strategy[3], published in 2020, reinstates the importance of trust and resilience in the Union, to be sustained in the long run for societal purposes and at a systemic scale. Therefore, cybersecurity risks and the capabilities for their mitigation need to be considered also from a systemic perspective. To this end, the analysis proposed in the report is based on a '**5G Ecosystem**' defined as a multi-dimensional space comprising not only 5G technological and functional domains but also the related technology lifecycle processes and stakeholders. The conceived ecosystem is also underpinned by a security dimension. The ecosystem and its components are described in detail in Section 2 *Scope, Definitions and Conventions.*

After having defined the '5G Ecosystem', the document:

- **collects** existing cybersecurity standards, specifications and guidelines, and **positions** them within the defined 5G ecosystem (Section 3 *Positioning and Assessment of Reference Documents in the 5G Ecosystem*);
- **identifies gaps in standardisation** by comparing the existing literature against an ideal situation of cybersecurity robustness and resilience, where standardisation addresses the necessary technical and organisational security aspects; and (Section 4 *Identification of Gaps in Standardisation*).

[2] Section 2.2 explains the taxonomy used by the document. For convenience the report refers to the documents analysed as, alternatively, 'reference documents', 'references', 'existing literature' or 'standards, specifications, guidelines'.
[3] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

- **formulates recommendations** on standardisation in the area of 5G cybersecurity (Section 5 *Recommendations*).

1.3 TARGET AUDIENCE AND PREREQUISITES

This work is intended for the stakeholders in the 5G ecosystem, in particular standardisation working groups, industry stakeholders and national cybersecurity agencies across the European Union.

The reader is invited to get familiar with the concepts of information security risk management as documented in the ISO/IEC 27005 international standard, as well as the concepts developed in the following documents:

- ENISA, Guideline on Security Measures under the EECC, 2020,
- ENISA, 5G Supplement to the Guideline on Security Measures under EECC, 2021,
- ENISA, Threat Landscape for 5G Networks, 2019,
- ENISA, Security in 5G Specifications, 2021,
- ENISA, EU Coordinated Risk Assessment of 5G Networks Security, 2019,
- ENISA, Methodology for Sectoral Cybersecurity Assessments, 2021.

An overview of the standardisation organisations active in 5G is contained in ENISA report ‘Security in 5G specifications’[4].

[4] https://www.enisa.europa.eu/publications/security-in-5g-specifications

2. SCOPE, DEFINITIONS, AND CONVENTIONS

This section provides the concepts and definitions used to build the ‘5G Ecosystem’ introduced in Section *1.2 Overview and Structure of the Study*. This ecosystem provides a methodological framework in which it is possible to locate the standards, the specifications and the guidelines relevant for a given stakeholder group, at a given step of the technology lifecycle, for a given block of the 5G technical architecture.

2.1 THE 5G ECOSYSTEM

As introduced in section *1.2 Overview and Structure of the Study*, the 5G ecosystem is composed of the following dimensions.

Figure 1: The dimensions of the 5G ecosystem

Building blocks of the 5G Ecosystem	Definitions
5G Technological and functional domains	Essential functions of 5G networks and the related supporting asset categories, representing 5G technical components and the scope of their interactions.
Technology lifecycle processes	Processes applied to the lifecycle of 5G services and of 5G-dependent vertical industrial processes.
5G Stakeholders	Entities (either public or private) that are related to 5G networks and vertical industries.
5G Security domains, objectives and measures	Security dimension of the 5G ecosystem, represented through the security domains, objectives and measures of the *ENISA Guideline on Security Measures under the EECC* and its 5G supplement.

2.1.1 5G technological and functional domains

The current section outlines the essential functions of 5G networks and the related categories of supporting assets considered in this report.

The 5G technological and functional domains considered are largely based on the set of planes, functional blocks and process blocks of the widely acknowledged representation of the generic 5G architecture depicted in the ENISA report *ENISA Threat Landscape for 5G Networks Updated 2020*, which in turn relies on the architecture of the 3GPP Technical Specification 23.502 (Release 16). They have been selected because they offer a synthetic overview of 5G technology and 5G-related processes. For the purpose of this study, only the major blocks depicted in Figure 2 have been considered.

Figure 2: The 5G technological and functional domains as represented in *ENISA Threat Landscape for 5G Networks Updated 2020*

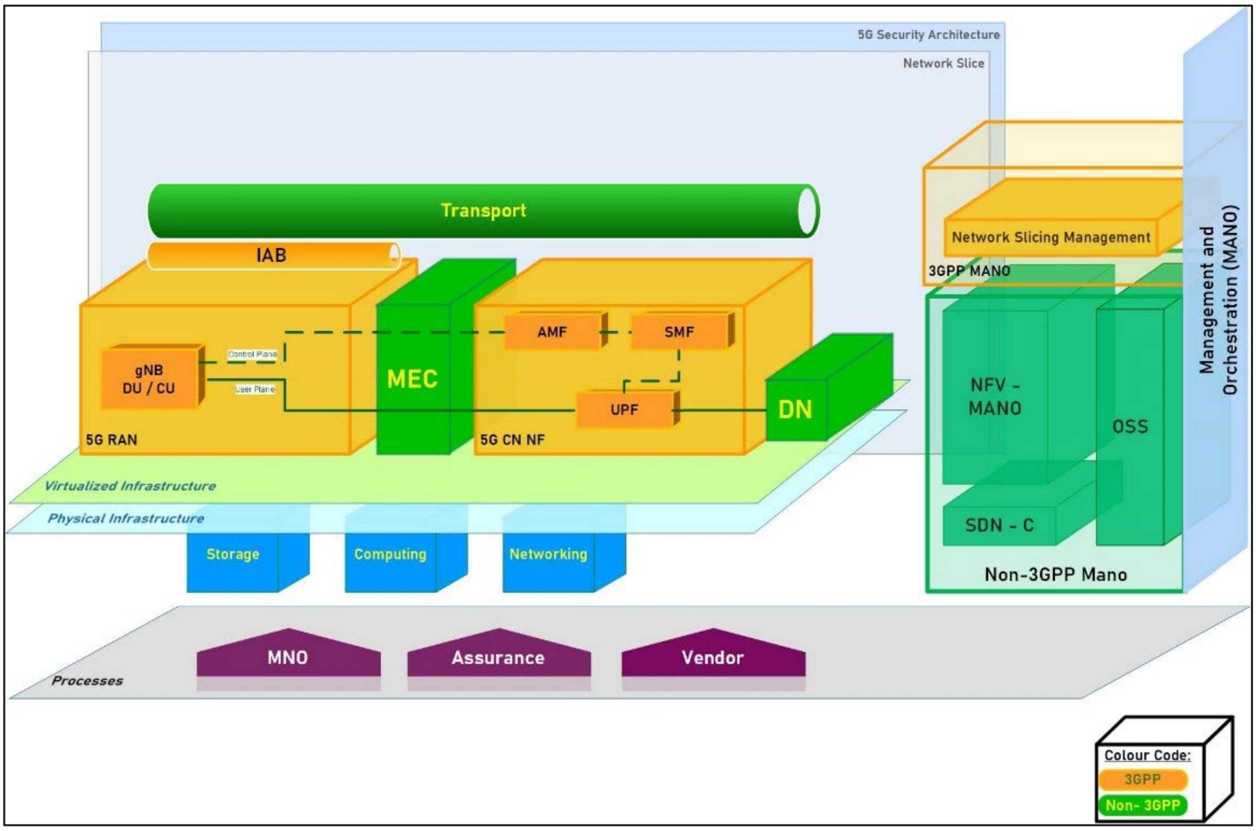


Figure 3: The 5G technological and functional domains considered by the current study

G Technical and functional domains	Definition
5G Use Cases	End-to-end services based on 5G, characterised by how they use and/or transmit data. Example: ‘Vehicle-to-everything’, eMBB, mMTC, URLLC.
Multi Access Edge Computing (MEC) Services	Multi-access computing services used to bring computation and connectivity closer to the end-user in order to meet the requirements for data transmission speed and latency.
Physical infrastructure	Set of premises including hardware and software for computation, storage, transmission, as well as the related technical environment (energy, air conditioning, cable paths, civil works infrastructures, etc.).
Virtualised Infrastructure	Computing, storage and networking capacities on demand.
Radio Access Network (RAN)	Logical and hardware components making up the functions of the radio access network. It includes mainly distribution units and control units for radio access.
Multi Access Edge Computing (MEC) Infrastructure	Infrastructure related to the decentralisation of cloud functions (storage of data and computing) located closer to the user or edge device.
5G Core Network, Network Function (CN NF)	Central part of the 5G infrastructure which enables new functions related to multi-access technologies. Its main

	purpose is to deliver services over all kinds of networks (wireless, fixed, converged).
Data Network (DN)	Connectivity to external data, content, services and other resources available outside the 5G network. The data network is also used to interconnect different 5G networks, operators and providers.
Transport	Part of the network ensuring the connectivity between the access and core networks.
Management and Orchestration (MANO)	Software, operations tools and the related environment used to automate operations that relate to the lifecycle of the infrastructure and service components.

2.1.2 Technology lifecycle processes

Lifecycle processes can be regarded as the heartbeat of all activities based on digital technologies. This section defines the scope of the technology lifecycle processes considered in the 5G ecosystem. They are the processes related to the lifecycle of 5G services and of 5G-dependent vertical industries. To keep the analysis simple, the methodology selects some of the processes listed in GSMA, GSMA FS.16 - NESAS Development and Lifecycle Security Requirements v2.0, 2021.

Such processes are considered in a technology environment including (but not limited to):

- 5G technologies given their underlying technological bricks from cloud-native and service-based architectures,
- their orchestration and their automation,
- their components running on top of virtualised infrastructures requiring orchestration and automation.

The considered processes encompass the phases shown in Figure 4 below.

Figure 4: The phases of the technology lifecycle processes considered in the 5G ecosystem

Phase	Definition
Think	All activities related to the design of a service, the design principles of an infrastructure, as well as the study of their technological and operational options. The main deliverables of this phase are (for example) anticipation studies, benchmarks, opportunity studies, high-level designs and initial risk assessments.
Build	All activities that prepare and execute the building phase of a service, including the integration of the software parts, connectivity, application interfaces, data flows and related protocols. When security is integrated within the 'Build' process, the corresponding milestones consist in checking the robustness of the architecture, its attack surface and updating the risks accordingly.
Test	All activities that verify the compliance with specifications, robustness or resilience prior or after the 'go-live' phase, also including auditing at any phase of the lifecycle.
Run	All activities including the continuous delivery of services, performance and fault management, problem management, customer support, etc.
Update	Activities that relate to the process also referred to as 'Transition', consisting in identifying capacity needs, requirements for software updates, patch installation, needs for robustness, adjustments to software and equipment

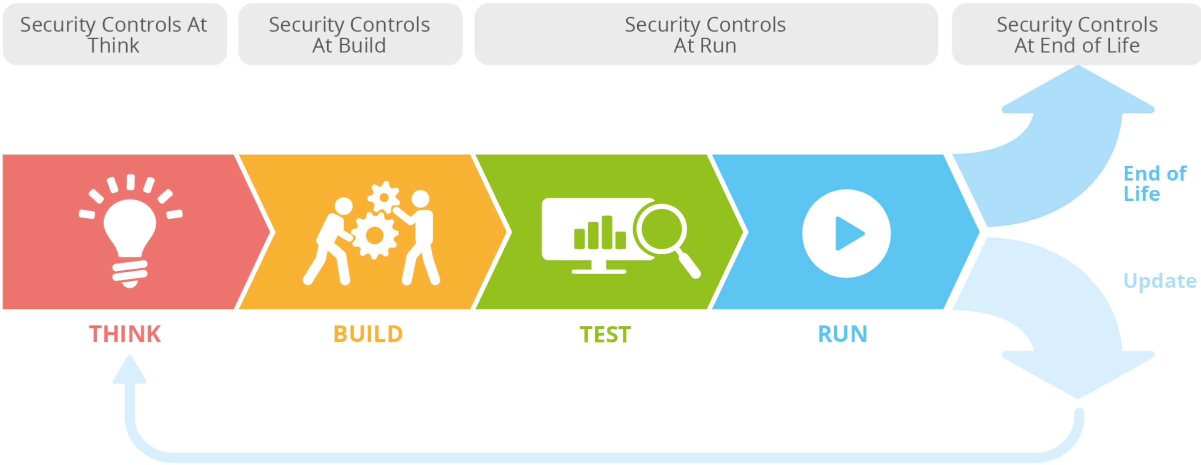
	configurations, and the on-demand provisioning capabilities when a customer purchases a service.
End of Life	The sequence of steps towards decommissioning or the end of the lifecycle of a service component.

In this context, it is to be noted that the lifecycle processes apply to a variety of areas and stakeholders beyond 5G products alone. These lifecycle processes are applicable to systems other than 5G products, such as IT systems used to operate, test, orchestrate, automate, and develop service bricks.

The figure below is an example showing where security steps can be implemented in the lifecycle processes to enable robustness and resilience from an end-to-end perspective.

Figure 5: Representation of the lifecycle processes considered in the 5G ecosystem

2.1.3 5G Stakeholders


Security Controls At Think
Security Controls At Build
Security Controls At Run
Security Controls At End of Life
End of Life
Update
THINK
BUILD
TEST
RUN

The 5G ecosystem relies on several stakeholders that play different roles in its security at different levels. The set of stakeholders selected for this document focuses on entities (either public or private) that are related to 5G networks and vertical industries.

The set has been adapted from the EU Coordinated Risk Assessment on 5G Networks Security and the ENISA Threat Landscape for 5G Networks Updated (2020), as they encompass both the stakeholders and their role with regards to 5G. They are depicted in the following table.

Figure 5: The categories of the 5G stakeholders considered in the 5G ecosystem

Stakeholder category	Definition
5G Service customer or consumer	Entities that use services that are offered by a service provider (SP): in the context of 5G, these would be, for example, vertical industries and their private networks. In addition, consumers of 5G services without a business-relation with a 5G service provider (for example, end users) are included in this category. **This category may implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services.**

Telecommunications sector (Telecom)	This category encompasses entities that are responsible for the manufacture, deployment and operation of 5G networks, such as: • Mobile Network Operators (MNOs): entities providing mobile network services to users, operating their own network, if necessary with the help of third parties • Suppliers of mobile networks: entities providing services or infrastructure to MNOs in order to build and/or operate their networks (both telecom equipment manufacturers and other third-party suppliers, such as cloud infrastructure providers and network infrastructure providers and managed services providers) • Service providers (SP): entities that design, build and operate services using aggregated network services. Examples include communication service providers offering traditional telecom services, digital service providers offering digital services such as enhanced mobile broadband and IoT to various vertical industries, or network slice as a service (NSaaS) providers offering a network slice along with the services that it may support and configure. • Virtualisation infrastructure service providers (VISP): entities that provide virtualised infrastructure services and design, build, and operate virtualisation infrastructure(s). The infrastructure comprises networking (e.g. for mobile transport) and computing resources (e.g. from computing platforms). **This category may implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services.**
Datacentre services providers (DCSP)	Entities that provide data centre services and that design, build and operate their data centres. A DCSP differs from a VISP by offering 'raw' resources (i.e. host servers) in rather centralised locations and simple services for consumption of these raw resources. A VISP rather offers access to a variety of resources by aggregating multiple technology domains and making them accessible through a single API. **This category may implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services.**
Connected devices industry	This category includes manufacturers of connected devices and related service providers, meaning entities providing objects or services that will connect to 5G networks (e.g. smartphones, connected vehicles, e-health) and related service components hosted in a 5G control plane as defined in a service-based architecture or mobile edge computing. **This category may implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services.**
Cybersecurity assessment	This category includes entities that assess the security of 5G networks and systems e.g. auditing companies and accredited 5G laboratories. **This category audits the implementation of standards, specifications and guidelines.**
Cybersecurity information exchange	This category includes entities that share threat intelligence and incident-related information, for example information sharing and analysis centres (ISACs) and cyber security incident response teams (CSIRTs).

	This category may implement standards, specifications and guidelines to securely exchange cyber-intelligence.
Standards development organisations (SDOs), associations, alliances	**This category encompasses entities that develop and promote the adoption of standards, specifications and guidelines**, for example, GSMA and 3GPP.
Research and innovation organisations	This category encompasses entities contributing to R&D and innovation tasks related to all kinds of innovative actions in areas related to 5G, including verticals. It also includes open source organisations or communities providing technological support and guidance in the development of 5G functions and services, as well as public-private partnerships and innovation programmes. **This category exposes gaps in standardisation and creates innovations that can lead to advancements in standardisation by acting as starting points of new standards, specifications and guidelines.**

Explanatory notes:

- 5G vertical industries working at the 'Think' phase of the lifecycle have been included in the category 'Research and innovation organisations'.
- 5G vertical industries using 5G services have been considered as service customers, whereas verticals delivering services to the customers in their own sector have been considered as service providers.
- Open-source organisations have been included in the category 'Research and innovation organisations' when considered for their development activities at the 'Think' phase of the lifecycle. They have been included in the category 'Suppliers of MNOs' when considered for their support to technologies in production.

2.1.4 5G Security domains, objectives and measures

This section outlines the security dimensions of the 5G ecosystem used in this report. In the absence of an equally comprehensive framework, the report uses the security domains, objectives and measures found in the *ENISA Guideline on Security Measures under the EECC* and its *5G supplement*. The former concern security in general, the latter concern 5G. Although they target mainly operators, the domains and measures set out in the documents above have been used as an analytical framework. Still, it is important to stress that the security measures used are not to be considered as the totality of the measures necessary for the mitigation of cybersecurity risks in 5G. Security objectives and measures could be added for any sectoral risk assessment covering a subset of the 5G ecosystem. The table below shows the security domains and objectives taken into consideration. The mapping of the reference documents is further broken down into security measures in Annex 6 *Detailed mapping*.

Figure 6: Security domains and objectives in the *Guideline on Security Measures under EECC and its 5G Supplement*

Security domains (D)	Security objectives
D1 – Governance and risk management	• Information security policy • Governance and risk management • Security roles and responsibilities • Security of third-party dependencies
D2 – Human resources security	• Background checks • Security knowledge and training • Personnel changes

	• Handling violations
D3 – Security of systems and facilities	• Physical and environmental security • Security of supplies • Access control to network and information systems • Integrity of network and information systems • Use of encryption • Protection of security critical data
D4 – Operations management	• Operational procedures • Change management • Asset management
D5 – Incident management	• Incident management procedures • Incident detection capability • Incident reporting and communication
D6 – Business continuity management	• Service continuity strategy and contingency plans • Disaster recovery capabilities
D7 – Monitoring, auditing, and testing	• Monitoring and logging policies • Exercise contingency plans • Network and information systems testing • Security assessments • Compliance monitoring
D8 – Threat awareness	• Threat intelligence • Informing users about threats

2.2 TAXONOMY OF DOCUMENTS CONSIDERED

To facilitate the analysis, this report relies on a taxonomy comprising three categories of documents. Each of the documents considered is assigned to one of the categories below, according to its related definition:

- **Standard**: *a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory*[5]. The standards considered are documents produced by a standardisation body (international, national or European), and whose content include (but is not limited to) requirements, principles, description of frameworks or processes and codes of practice.
- **ICT Technical specification**: *a technical specification in the field of information and communication technologies*[6]. ICT technical specifications are referred in this document as 'specifications'.
- **Guidelines and Best Practices**: documents that *explain, interpret and simplify […] standards or […] standardisation deliverables*. These can include *user guides, abstracts of standards, best practice information and awareness-building actions, strategies, and training programmes*[7].

For convenience, the report refers to the documents analysed as, alternatively, 'reference documents', 'references', 'existing literature' or 'standards, specifications and guidelines.

[5] Standardisation bodies as defined by Regulation (EU) No 1025/2012, 2012), Article 2 paragraph (1)
[6] Understood as 'ICT technical specification' as defined by Regulation (EU) No 1025/2012, 2012), Article 2 paragraph (5)
[7] Definition adapted from Regulation (EU) No 1025/2012, 2012) Chapter IV, Article 15, paragraph 1 Alinea (f). The reference to 'European' standards and standardisation deliverables has been deleted as the current report refers also to non-European documents.

Although these categories have been identified solely for the purpose of the study, they are based on the EU Regulation on European standardisation (Regulation (EU) No 1025/2012, 2012) and of the International Standardisation Organisation (ISO). A reminder of the exact definitions is given in Annexes 1 and 2 on the taxonomy for standards.

Cybersecurity standards provide an important range of contents: requirements applicable to ICT-related domains of technology or processes, requirements for management systems, frameworks and guidelines on security controls about ‘what’ to do.

In turn, reference documents helping the implementation and the ‘how’ to do things relate to specifications, guidelines, and best practices.

The documents analysed in this report are listed in the Annex 5 *Referencing the Existing Literature*. An important part of the 5G-related documents in this study are referred in the report from ENISA *Security in 5G Specifications* (2021).

3. POSITIONING AND ASSESSMENT OF REFERENCE DOCUMENTS IN THE 5G ECOSYSTEM

3.1 METHODOLOGY FOR THE ASSESSMENT OF COVERAGE

This section provides the methodology to position existing standards, specifications and guidelines in the 5G ecosystem and to assess the extent to which they address the 5G security environment. It consists of the following steps:

- Using ENISA's literature and complementary knowledge of the Expert Group missioned for this study, relevant documents are sampled and grouped into consistent clusters ('shorthand') made up of a selection of standards, specifications, and guidelines. The documents analysed are listed in the Section 6 *Bibliography.*
- These clusters are mapped against each security domain, objective and measure of the 5G ecosystem as described Section 2.1.4 *5G Security domains, objectives and measures*.
- The relevance and the completeness of the clusters is then analysed from the perspectives of the three remaining dimensions of the 5G ecosystem, that is its stakeholders (Section 2.1.3 *5G Stakeholders*); its technical and functional domains (Section 2.1.1 *5G technological and functional domains*); and the related technology lifecycle processes (Section *2.1.2 Technology lifecycle processes*).
- The results of the mapping and of the assessment are described in the section Annex 6 *Detailed Mapping*. A summarised version is contained in section *3.2 Consolidated Results*.

3.2 CONSOLIDATED RESULTS

The detailed analysis underlying this report concerns more than 150 security measures and more than 140 documents which were identified and selected from the available literature. This detailed and in-depth analysis is provided in section Annex 6 *Detailed Mapping*.

Given the volume of information and the level of detail, the current section only contains a summary table, representing the consolidated findings by security domain. A high-level assessment of the extent to which the analysed literature addresses a given security domain for each of the dimensions of the 5G ecosystem (i.e. stakeholders, technological and functional domains, and technology lifecycle processes) is also provided.

Some details may not be obvious in the consolidated results. For example, 'All' under the column 'Coverage of Stakeholders' means that the literature analysed is considered relevant for every entity in the ecosystem. The specific degree or depth of relevance for each category of stakeholders, technological and functional domains, and technology lifecycle processes is tackled in the detailed mapping.

Figure 7: Summary of the coverage of existing literature by security domain

Security domain	Taxonomy of applicable documents	Coverage of the dimensions of the 5G ecosystem			Observations
		Stakeholders	5G Technological and functional domains	Technology lifecycle processes	
D1 – Governance and risk management	Standards	All	All	All	The documents referred to are, to some extent, relevant to all dimensions of the 5G ecosystem. However, they are not specific to 5G. To get their full value, each stakeholder category would need to put in a significant effort to tailor them to the relevant 5G technical and functional domains and technology lifecycle processes. Such an effort requires skills and expertise. Furthermore, fragmentation in implementation should be avoided.
D2 – Human resources security	Standards	All	All	All	The documents referred to are to some extent relevant to all dimensions of the 5G ecosystem. However, they are not specific to 5G. To get their full value, each stakeholder category would need to put in a significant effort to tailor them to the relevant 5G technical and functional domains and technology lifecycle processes. Such an effort requires skills and expertise. Furthermore, fragmentation in implementation should be avoided
D3 – Security of systems and facilities	Standards Specifications Guidelines	Telecommunications sector DCSPs	All	Run	Although general, the documents referred to are especially relevant for the telecommunications sector and DCSPs. Also, they are relevant to all technological and functional domains. They can be tailored with minimal effort to a 5G-specific context in the 'Run' phase. Tailoring to the 'Think' and 'Build' phases would require significant effort by the stakeholders.
D4 – Operations management	Specifications	Telecommunications sector	All	Run	The documents referred to are not specific to 5G, although especially relevant for the telecommunications sector. To get their full value, each stakeholder category would need to put in a significant effort to tailor them to the relevant 5G technical and functional domains and technology lifecycle processes (at the 'Think' and 'Build' phases). Such an effort requires skills and expertise. Furthermore, fragmentation in implementation should be avoided.
D5 – Incident management	Standards	Telecommunications sector	All	Run	The documents referred to are not specific to 5G, although especially relevant for the telecommunications sector. To get their full value, each stakeholder category would need to put in a significant effort to tailor them to the relevant 5G technical and functional domains and technology lifecycle processes (at the

					‘Think’ and ‘Build’ phases). Such an effort requires skills and expertise. Furthermore, fragmentation in implementation should be avoided.
D6 – Business continuity management	Standards	Telecommunications sector	All	Run	The documents referred to are not specific to 5G, although especially relevant for the telecommunications sector. To get their full value, each stakeholder category would need to put in a significant effort to tailor them to the relevant 5G technical and functional domains and technology lifecycle processes (at the ‘Think’ and ‘Build’ phases). Such an effort requires skills and expertise. Furthermore, fragmentation in implementation should be avoided.
D7 – Monitoring, auditing, and testing	Standards	Telecommunications sector	All	Run	The documents referred to are not specific to 5G, although especially relevant for the telecommunications sector. To get their full value, each stakeholder category would need to put in a significant effort to tailor them to the relevant 5G technical and functional domains and technology lifecycle processes (at the ‘Think’ and ‘Build’ phases). Such an effort requires skills and expertise. Furthermore, fragmentation in implementation should be avoided.
D8 – Threat awareness	Guideline	Telecommunications sector	All	Run	The documents referred to are not specific to 5G, although especially relevant for the telecommunications sector. To get their full value, each stakeholder category would need to put in a significant effort to tailor them to the relevant 5G technical and functional domains and technology lifecycle processes (at the ‘Think’ and ‘Build’ phases). Such an effort requires practice. Furthermore, fragmentation in implementation should be avoided.

4. IDENTIFICATION OF GAPS IN STANDARDISATION

4.1 METHODOLOGY FOR THE IDENTIFICATION OF GAPS IN THE EXISTING LITERATURE

This section presents existing literature addressing each security domain in accordance with Section 2.1.4 *5G Security domains, objectives and measures* from the perspective of the stakeholder considered in accordance with Section 2.1.3 *5G Stakeholders* and points to the areas partly covered by existing literature as well as those covered to a limited extent or not at all.

The identification of these areas relies on expert assessment by the authors of this report. They have assessed the extent to which the existing literature addresses an 'ideal situation' where 5G technical and organisational cybersecurity risks are mitigated and adequate controls to ensure security are performed thanks to available standards, specifications, and guidelines. This is therefore the reference against which gaps in standardisation have been identified.

4.2 ASSESSMENT OF COVERAGE AND IDENTIFICATION OF GAPS IN STANDARDISATION

The assessment of the coverage of the standards, specification and guidelines considered, as well as the identification of the gaps in standardisation, is conveyed in the form of a table (Figure 9), which follows the colour coding below:

Figure 8: Colour coding for the representation of the gaps

Colour code	Definition
🟩	**Existing literature** The green cells show the existing literature addressing each security domain from the perspective of the stakeholder considered.
🟨	**Moderate Gap** The yellow cells indicate the areas where moderate gaps in standardisation have been identified. A gap is identified as 'moderate' when the existing literature addresses the domain partly, meaning that moderate effort would be required to bridge that gap.
🟧	**Major gap** The orange cells indicate the areas where major gaps in standardisation have been identified. A gap is identified as 'major' when the existing literature does not address the domain (or only to a limited extent), meaning that a major effort would be required to bridge that gap.
	No gap/Not relevant The cells that are not coloured indicate areas where no gaps have been identified or only those that are not relevant for the stakeholder.

For research and innovation organisations, gaps are intended as areas where further work by these organisations is required.

For every domain, the table (Figure 9) identifies between brackets the relevant literature as grouped by the shorthand in Annex 5 *Referencing the existing literature*, reproduced below for convenience.

Figure 9: Reference shorthand – each shorthand indicates the areas covered by the selection of documents

Shorthand	Selection of documents concerning:
ISOIEC27K	ISO/IEC 27K series
ISOIEC20K	IT services process map
SUPPLSEC	Security of suppliers
POLTEMPLATES	Build security policies
RM	Cybersecurity risk management
ENISATL	ENISA works related to threats
SP800HR	Security related to human resources
IAM	Identity and access management.
DEVSECOPS	Security in the IT lifecycle
3GPP-All	3GPP technical specifications
NFVSEC	Security of network functions virtualisation
eUICC	Security in the eUICC domain
CRYPTOTECH	Use of cryptographic techniques
PHYSEC	Physical and environmental security
HARDEN	Technical robustness
VULN	Management of vulnerabilities
THREATMOD	Threat modelling and security monitoring
SECASSUR	Security assurance and related guidelines
AUDIT	Audit planning and assessment
BCM	Organisational and technical resilience

Figure 10: Assessment of coverage and evaluation of gaps in standardisation

	Stakeholders	**5G Service customer or consumer**	**Telecom sector**	**Datacentre Services Providers**	**Connected devices industry**	**Cybersecurity assessment stakeholders**	**Cybersecurity information exchange stakeholders**	**Research and innovation organisations***
	Role in standardisation	**Implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services**				**Audit the implementation of standards, specifications and guidelines**	**Implement standards, specifications and guidelines to securely exchange cyber-intelligence**	**Expose gaps in standardisation and create innovations that can lead to advancements in standardisation, by acting as starting points for new standards, specifications and guidelines**
D1 **Governance and risk management**	**Existing literature addressing the domain**	[ISOIEC27K], [ISO20K], [RM], [SP800HR], [ENISATL], [ISOIECSUPPL], [POLTEMPLATES]				[SECASSUR]	[RM]	[RM] [NFVSEC] [DEVSECOPS], [HARDEN]
	Moderate gap: **Areas partly covered by existing literature**	• Sector-specific governance and risk management • Sector-specific risk register • Sector-specific ISMS and PIMS implementation				5G risk assessment by third parties	Processes for cross-border information exchange to share best practices in governance and risk management	
D2 **Human resources security**	**Existing literature addressing the domain**	[SP800HR], [IAM]				[SP800HR]	[SP800HR]	[ISOIEC27K], [SP800HR], [IAM]
	Moderate gap: **Areas partly covered by existing literature**	Vertical-specific educational security content, specifying awareness programmes and training contents e.g. MOOCs, serious games services (*note: area that might be addressed by soft measures, not standards*)				Evaluation methods of human resources management processes	Cross-border process for the exchange of information (e.g. best practices) on the security of human resources	Vertical-specific educational security content, specifying awareness programmes and training contents e.g. MOOCs, serious games services**
D3 Security of systems and facilities	**Existing literature Addressing the domain**	**[PHYSEC], [IAM], [3GPP-AII], [SECASSUR], [CRYPTOTECH], [NFVSEC], [eUICC]**				**[AUDIT], [SECASSUR]**		**[DEVSECOPS], [eUICC], [CRYPTOTECH]**

	Moderate gap: **Areas partly covered by existing literature**	- Robust configuration and deployment of 5G vertical use cases - Robust configuration of 5G micro services and automation - Security of RAN, Open RAN, ONAP		- Methods for evaluating the security of 5G verticals - Methods for evaluating the robustness of the configuration of 5G micro services and automation		- Testbeds environments and tools**
	Major gap **Areas not covered (or covered to a limited extent) by existing literature**	- Information security requirements applicable to vendors of 5G solutions sourcing contracts - Automation of robust configurations and deployment		Audits of the security of orchestration and micro-services (*note: area that might be addressed by soft measures, not standards*)		
D4 Operations management	**Existing literature addressing the domain**	**Standards [ISO20K], [RM], [NFVSEC]**		**Standards [ISO20K], [RM], [AUDIT]**		**[DEVSECOPS]**
	Moderate gap: **Areas partly covered by existing literature**	High-level requirements for 5G-specific cloud-native and edge deployments	Operations and security practices concerning firmware, data aggregation and related components	Third party risk assessment of 5G operations		
	Major gap **Areas not covered (or covered to a limited extent) by existing literature**	Requirements to implement the whole lifecycle of 5G-specific cloud-native and edge deployments such as: centralised management of certificates, interoperable automation and orchestration, serverless environments	Automated security evaluation for industrial IoT			- Testbeds environments and tools**
D5 **Incident management**	**Existing literature addressing the domain**	**[ISOIEC20K], [ISOIEC27K], [BCM], [AUDIT]** **[THREATMOD], [NFVSEC]**		**[ISOIEC20K], [ISOIEC27K], [BCM], [AUDIT]**	**[ISOIEC20K], [ISOIEC27K], [BCM], [AUDIT]**	**[DEVSECOPS]**

	Moderate gap: **Areas partly covered by existing literature**	- Typologies of scenarios for 5G-specific, end-to-end incident management, including severity criteria and thresholds for incidents in a 5G context	Evaluation methods for the investigation of incidents and the chain of custody for evidence	- Typologies of scenarios for 5G-specific, end-to-end incident management, including severity criteria and thresholds for incidents in a 5G context - Processes for cross-border information exchange to share best practices in incident response	
	Major gap **Areas not covered (or covered to a limited extent) by existing literature**	- Automated incident response in a 5G context	Evaluation methods for the performance of automated incident response		
D6 **Business continuity management**	**Existing literature addressing the domain**	**[ISOIEC27K], [VULN], [BCM]**	**[ISOIEC27K], [VULN], [BCM], [AUDIT]**	**[ISOIEC27K], [BCM], [AUDIT]**	
	Moderate gap: **Areas partly covered by existing literature**	- 5G-specific business impact analysis - Methodology to assess ICT readiness - 5G-specific disaster recovery		- Processes for cross-border information exchange to share best practices in business continuity	
	Major gap **Areas not covered (or covered to a limited extent) by existing literature**	- Technical disaster recovery plans for 5G functions and orchestration	Methods for evaluating the ICT ICT readiness for business continuity		
D7 Monitoring, auditing and testing	**Existing literature Addressing the domain**	**[VULN], [HARDEN],[THREATMOD], [DEVSECOPS]**	**[AUDIT]**		**[DEVSECOPS]**

	Moderate gap: **Areas partly covered by the existing literature**		• Evaluation methods for monitoring capabilities • Evaluation methods for the capabilities of automated testbeds	Process for the cross-sector exchange of information in the area of sharing best practices for monitoring, auditing and testing	
	Major gap **Areas not covered (or covered to a limited extent) by existing literature**	• 5G-specific log sources • Event correlation for 5G end-to-end services and roaming			
D8 **Threat awareness**	**Existing literature addressing the domain**	**Knowledge base of risk sources, attack methods, best practices of incident playbooks [THREATMOD], [ISOIEC27K], [RM], [SECASSUR]**	**[THREATMOD]**	**[THREATMOD]**	**[DEVSECOPS], [eUICC], [CRYPTOTECH]**
	Moderate gap: **Areas partly covered by the existing literature**	Typologies of threats for 5G-verticals applicable to RAN / Open RAN, APIs, ONAP, and cloud native technology	Evaluation methods for the capabilities of the effectiveness of threat intelligence and threat hunting	Process for the cross-sector exchange of information in the area of sharing threat intelligence	• Prerequisites for standards: new specifications, testbeds environments and tools
	Major gap **Areas not covered (or covered to a limited extent) by existing literature**	Automatic remediation playbooks			

* *Note: For research and innovation organisations, gaps are intended as areas where further work by these organisations is required.*

*** Note: area that might be addressed by soft measures, not standards.*

4.3 OVERVIEW OF GAPS BY SECURITY DOMAIN

The gaps identified in the previous table can be summarised as follows:

Security domain	Moderate gaps	Major gaps
D1 – Governance and risk management	• Sector-specific governance and risk management • Sector-specific risk register • Sector-specific ISMS and PIMS implementation • 5G risk assessment by third parties • Processes for cross-border information exchange to share best practices in governance and risk management	
D2 – Human resources security	• Vertical-specific educational security content, specifying awareness programmes and training contents e.g. MOOCs, serious games services (*note: area that might be addressed by soft measures, not standards*). • Methods for evaluating the management processes for human resources • Cross-border process for the exchange of information (e.g. best practices) on the security of human resources	
D3 – Security of systems and facilities	• Robust configuration and deployment of 5G vertical use cases • Robust configuration of micro services and automation • Security of RAN, Open RAN, ONAP	• Information security requirements applicable to vendors of 5G solutions sourcing contracts • Automation of robust configurations and deployment • Audits of the security of orchestration and micro-services (*note: area that might be addressed by soft measures, not standards*)

	• Methods for evaluating the security of 5G verticals • Methods for evaluating the robustness of the configuration of 5G micro services and automation	
D4 – Operations management	• High-level requirements for 5G-specific cloud-native and edge deployments • Operations and security practices concerning firmware, data aggregation and related components • Third party risk assessment of 5G operations	• Requirements to implement the whole lifecycle of 5G-specific cloud-native and edge deployments such as centralised management of certificates, interoperable automation and orchestration, serverless environments • Automated of security evaluation for industrial IoT
D5 – Incident management	• Typologies of scenarios for 5G-specific, end-to-end incident management, including severity criteria and thresholds for incidents in a 5G context • Evaluation methods for the investigation of incidents and the chain of custody for evidence • Processes for cross-border information exchange to share best practices	• Automated incident response in a 5G context • Evaluation methods for the performance of automated incident response
D6 – Business continuity management	• 5G-specific business impact analysis • Methodology to assess ICT readiness • 5G-specific disaster recovery • Processes for cross-border information exchange to share best practices in business continuity	• Technical disaster recovery plans for 5G functions and orchestration • Methods for evaluating the ICT readiness for business continuity
D7 – Monitoring, auditing, and testing	• Evaluation methods for monitoring capabilities • Evaluation methods for the capabilities of automated testbeds	• 5G-specific log sources • Event correlation for 5G end-to-end services and roaming

	• Process for the cross-sector exchange of information in the area of sharing best practices for monitoring, auditing and testing	
D8 – Threat awareness	• Typologies of threats for 5G-verticals applicable to RAN / Open RAN, APIs, ONAP, and cloud native technology • Evaluation methods for the capabilities of the effectiveness of threat intelligence and threat hunting • Process for the cross-sector exchange of information in the area of sharing threat intelligence	• Automatic remediation playbooks

4.4 OBSERVATIONS ON THE GAPS IN STANDARDISATION

The gap analysis is based on the standards, specifications and guidelines presented in Section *6 Bibliography*.

The following should be noted.

- The bibliography relies on a sampled set of documents. Despite the authors' efforts, there may exist standards, specifications or guidelines that are not referenced and thus a gap is reported in error.
- When a partial or major gap is pointed out, the question arises as to whether this area should be standardised, supported by specifications or guidelines, or whether company-specific needs make this contextualisation impossible.

Given the above, the present report might over-represent existing gaps in some areas. For example, in relation to the latter point, one consistent observation is that the lifecycle of open-source software does not fit well with the processes defined in the standards, specifications, and guidelines. This is mainly due to the lack of a formal organisational structure that could support, enforce and finance standardised processes in the open-source community. This is particularly true for the security domains D1 (Governance and Risk Management), D7 (Monitoring, Auditing and Testing) and D8 (Threat Awareness).

Furthermore, the process for developing security standards is not included in the analysis itself. The interests of individual players may influence the definition of security standards, specifications, or guidelines in favour of economic or other trade-offs – sometimes at the cost of a higher risk. One example is the trade-off between capabilities for legal interception and security against espionage through end-to-end confidentiality.

4.5 ADDITIONAL LEARNINGS AND OBSERVATIONS

Complementary to the assessment of the coverage of the existing security literature, the following elements intend to bring a qualitative perspective on the organisational and technical areas where the 5G stakeholders can intervene to improve maturity, robustness, and readiness for resilience.

The following list gathers observations from the initial deployments of 4G that have been shared in the Telecom industry. These trends continue to be relevant and should be considered in the context of 5G[8]:

- The complexity of simultaneously operating virtualised infrastructure and virtualised network functions (VNFs) working together;
- The need for consistency between the three key technical domains of VNFs (Virtual Network Functions), SDN (Software-defined networks) controllers, IaaS (Infrastructure as a Service) due to their mutual dependencies;
- The reliance on a Linux kernel leading to a systemic risk related to unexpected changes of configuration or unexpected behaviours at the core of computing and connectivity capabilities, possibly impacting also new critical functions e.g. orchestration, containers and microservices;
- The emergence of new solutions to entrust data management on cloud-based and serverless solutions, based on short-lived assets requiring new approaches for the observability of actions and for detecting threats;
- New cloud environments impact identity and access management as they are no longer purely role-based, but attribute-based and context-based;
- The increased need for confidentiality and resilience on connectivity and data storage in the network and its operation;
- The exploding number of cryptographic certificates to ensure legitimacy and avoid man-in-the-middle attacks shine a new light on key management;
- The abundance of configurations using text-based descriptors such as JSON and XML, together with highly distributed processing and storage;
- The effects of the increased importance of IT technologies including the importance of open source, both at service and infrastructure levels;
- The large number of APIs bringing complexity in ensuring the legitimacy of requests and the balance between attack surface and the exposure of an application interface;
- Cybersecurity incidents involving the recurring exposure of credentials and secrets in CI/CD environments;
- The MNOs' tendency to outsource their network operations and field operations to third-party service providers entrusted with multiple networks in multiple countries, which reinforces the importance of connectivity and therefore the inter-dependency between the ability to operate and the operated assets;
- Outsourcing to 'tower companies' (companies taking charge of the radio access sites) and 'fibre companies' (companies that operate fibre access networks), which are now entrusted with managing several operators simultaneously in several countries.

The above key trends are observed in 4G, but they should be taken into consideration to improve the coverage of standardisation for the cybersecurity of 5G.

Furthermore, one should take into account the fact that 5G networks are 'systems of systems', whose representation requires automation and abstraction and whose services necessitate end-to-end quality controls.

[8] (Affirmed Networks, 2019)

5. RECOMMENDATIONS

This section provides the recommendations that result from the previous sections and in particular from the identification of gaps.

5.1 ADOPT A PROGRESSIVE APPROACH TO 5G STANDARDISATION

The report suggests that a progressive approach to 5G standardisation be undertaken. Such an approach should start by improving existing literature. The current report could help this effort as it gives an overview of references and assesses their suitability for a given security measure, technical and functional domain and/or stakeholder. The creation of new references – if needed – could be a subsequent step to enhance standardisation coverage.

5.2 HAVE A BROADER VIEW ON THE CREATION OF NEW REFERENCES

The creation of new standards, specifications and guidelines should consider several elements.

- *Usefulness and necessity*. It should be considered whether the creation of standards, specifications and guidelines is necessary and/or useful for a specific security measure, for a specific 5G domain, and/or for a specific stakeholder at a given stage of the lifecycle.
- *Link with strategic objectives*. It is recommended that a consistent link between any new reference and the strategic objective it should serve is ensured. For instance, if the objective of a new reference is to harmonise practices at the European level, local regulations should be taken into consideration. For example, contextualisation of HR (human resources) measures must account for local regulations. A special attention shall be brought to provisions for legal interception.
- *Measurability of effectiveness*. New references should facilitate the consistent measuring of the effectiveness of the security measures from an end-to-end service perspective.
- *Consideration for new technologies.* For example, detection tactics of incidents in 5G should be tackled also from the perspective of the development and operation of Artificial Intelligence, and not only from the standpoints of mobile network operators, their managed services provider, and B2B verticals.
- *Thinking beyond standardisation*. In some cases, the effectiveness of standards, specifications or guidelines depends on external factors. For example, because of the open nature of the development of free and open source software (FOSS), security guidelines and recommendations should be accompanied by the commitment of resources to development and audit. Therefore, industry players and public administrations relying on open source software should be encouraged to actively contribute to continuously improve and maintain the security of the FOSS-based solutions.

5.3 FOSTER THE MATURITY AND THE COMPLETENESS OF THE IDENTIFICATION AND ASSESSMENT OF RISK

Section *4 Identification of Gaps in Standardisation* points to areas, for each security domain, that are partly covered by the existing literature, as well as those covered to a limited extent or not at all. Besides these specific areas, the experts observed a broader gap related to risk assessment. The existing literature related to risk assessment is not specific to 5G and/or does not identify and evaluate risks consistently. This leads to a fragmented security landscape which might be detrimental for the overall security of 5G.

Therefore, it is important to foster the maturity and the completeness of risk identification and assessment, by harmonising risk assessment practices in a way that is inclusive of all stakeholders of the 5G ecosystem. For example, this would imply in particular (but not only) standardised:

- registers of risks, including from the perspective of the telecommunications sector and service customers,
- skills and capacities frameworks for third party assessment,
- knowledge bases of threat scenarios,
- requirements for security monitoring,
- assessment methods with an adequate abstraction level,
- requirements for auditing capability, in particular for service providers.

In this context, it is worth mentioning the approach to risk identification outlined in ENISA's *Methodology for Sectoral Cybersecurity Assessment*, and described in the subsequent section.

5.3.1 ENISA's methodology for sectoral cybersecurity assessment

The European Cybersecurity Act (CSA) obliges to the definition of security and certification requirements for ICT products, services and processes to be based on the risk associated with their intended use.

To this end, ENISA has proposed the SCSA methodology (ENISA *Methodology for Sectoral Cybersecurity Assessments*, 2021) to support the identification of cybersecurity risks associated with the intended use of systems in the context of business services and processes, with the option to involve all stakeholders from sectoral vertical users to the providers of network infrastructure. SCSA carries out the assessment at sectoral business level involving all relevant 5G stakeholders, their business objectives and their ICT subsystems and processes.

Cybersecurity risks are identified in relation to the business objectives and the risks identified indicate the security, certification and assurance level requirements for particular ICT products, services and processes. This can support a balance between the cost that a 5G stakeholder has to cover for security and assurance and the benefit of protecting his business objectives.

5.4 FINAL OBSERVATIONS

It is to be noted that the prioritisation of new references to be created is outside the scope of this work and that, in accordance with the previous recommendation, the creation of new references might not always be necessary and should be part of a progressive approach which should consider several aspects.

Finally, it is important to stress that, while the technical and organisational standards analysed can contribute to the security of 5G, they should not be treated as an exhaustive list of measures guaranteeing security. Besides considerations of the effectiveness of specific standards that are outside the scope this report, it should be reminded that there are risks that are not covered by standards, for example residual risks whose cost is neither borne by nor attributable to a specific stakeholder, such as societal risks resulting from network malfunctions.

The complexity of 5G, as depicted in the previous sections, calls for a comprehensive vision of trust and of resilience that goes beyond standardisation. This vision should be future-proof and not dependent on the variability of assets and configurations in the network.

6. BIBLIOGRAPHY

1. 3GPP (2016): 3GPP 33.117 Catalogue of general security assurance requirements; Technical Specification.
2. 3GPP (2016): 3GPP 33.401 3GPP System Architecture Evolution (SAE); Security architecture.
3. 3GPP (2020): 3GPP 33.102 3G security; Security architecture; Technical Specification.
4. 3GPP (2020): 3GPP 33.116 Security Assurance Specification (SCAS) for the MME network product class.
5. 3GPP (n.d.): 3GPP 33.163 Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST).
6. 3GPP (n.d.): 3GPP 33.210 Network Domain Security (NDS); IP network layer security.
7. 3GPP (n.d.): 3GPP 33.310 Network Domain Security (NDS); Authentication Framework (AF).
8. 3GPP. (n.d.): 3GPP 33.501 Security architecture and procedures for 5G System.
9. 3GPP. (n.d.): TS 33.514 - 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class.
10. ANSI. (2019); ANSI/TIA-569-E ‘Telecommunications Pathways and Spaces’.
11. ANSSI (2018): EBIOS Risk Manager; Paris ANSSI.
12. ASIS (2021): ASIS Physical Asset Protection Guideline; Retrieved from asis.org: https://www.asisonline.org/publications--resources/standards--guidelines/
13. Carder, J. (2020): How to build a SOC with limited resources.
14. Carder, J. (2020): Security Operation Centers Maturity Model.
15. CIS (2018): CIS Risk Assessment Method.
16. CIS (2021): CIS Controls® v8; Retrieved from https://www.cisecurity.org/controls/v8/
17. Cloud Security Alliance (2015); Best practices for mitigating risks in virtualized environments.
18. CSIAC (2021): CSIAC evaluation of threat taxonomies; Retrieved from https://csiac.org/articles/evaluation-of-comprehensive-taxonomies-for-information-technology-threats/
19. EBIOS C (2021): Oberisk; Retrieved from https://club-ebios.org/site/en/tag/oberisk-en/
20. ENISA (2014): Report on Cyber Crisis Cooperation and Management.
21. ENISA (2016): Threat Taxonomy; Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.
22. ENISA (2019): EU Coordinated Risk Assessment of 5G Networks Security.
23. ENISA (2019): Threat Landscape for 5G Networks.
24. ENISA (2020): ENISA Threat Landscape for 5G Networks Updated.
25. ENISA (2020): Guideline on Security Measures under the EECC.
26. ENISA (2021): 5G Supplement to the Guideline on Security Measures under EECC.
27. ENISA (2021): Methodology for Sectoral Cybersecurity Assessments.
28. ENISA (2021): Security in 5G Specifications.
29. ETSI (2014): ETSI GS NFV-SEC 003 - Network Functions Virtualisation (NFV) - NFV Security - Security and Trust Guidance.
30. ETSI (2014): Network Functions Virtualisation (NFV);Architectural Framework.
31. ETSI (2017): ETSI GS NFV-SEC 012 - Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components.
32. ETSI (2017): Network Function Virtualisation (NFV);Reliability; Report on the resilience of NFV-MANO critical capabilities.

33. ETSI (2017): Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification.
34. ETSI (2018): ETSI GS NFV-SEC 014 - Network Functions Virtualisation (NFV) Release 3 - NFV Security - Security Specification for MANO Components.
35. ETSI (2022): ETSI TS 103.465 Smart Secure Platform (SSP); Requirements Specification.
36. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.
37. Regulation (EU) 2019/881 - Cybersecurity Act; Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
38. European Commission (2020, December 16): Brussels, Belgium, EU Press Release; New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient.
39. Fédération Française des Télécoms (2019): Repository of security objectives for Virtualised Network Functions (French).
40. GSMA (2019): GSMA FS.11 - SS7 Interconnect Security Monitoring and Firewall Guidelines.
41. GSMA (2019): GSMA FS.19 - Diameter Interconnect Security.
42. GSMA (2020): GSMA FS.23 - Coordinated Vulnerability Disclosure; Guideline.
43. GSMA (2020): GSMA FS.37 - GPRS Tunnelling Protocol User Security.
44. GSMA (2020): GSMA NG.113 - 5G System Roaming Guidelines.
45. GSMA (2021): GSMA FS.16 - NESAS Development and Lifecycle Security Requirements v2.0.
46. GSMA (n.d.): PRD FS.04 GSMA SAS Standard for UICC Production.
47. GSMA (n.d.): PRD FS.05 GSMA SAS Methodology for UICC Production.
48. GSMA (n.d.): PRD FS.08 GSMA SAS Standard for Subscription Manager Roles.
49. GSMA (n.d.): PRD FS.09 GSMA SAS Methodology for Subscription Manager Roles.
50. GSMA (n.d.): PRD FS.18 GSMA SAS Consolidated Security Guidelines.
51. GSMA (n.d.): PRD SGP.01 Embedded SIM Remote Provisioning Architecture.
52. GSMA (n.d.): PRD SGP.02 Remote Provisioning Architecture for Embedded UICC; Technical Specification.
53. GSMA (n.d.): PRD SGP.21 Remote SIM Provisioning (RSP) Architecture.
54. GSMA (n.d.): PRD SGP.22 Remote SIM Provisioning (RSP) Technical Specification.
55. GSMA (n.d.): TS 33.513 - 5G Security Assurance Specification (SCAS); User Plane Function (UPF); Technical Specification.
56. GSMA (n.d.): TS 33.515 - 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class.
57. IETF (2004): IETF RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure.
58. Informationstechnik, B. F. (2017): BSI Standard 200-3 - IT Risk Management: Standard.
59. ISO (2010): ISO/IEC 11770-1:2010 - Information technology — Security techniques — Key management — Part 1: Framework.
60. ISO (2012): ISO/IEC 17024:2012 - Conformity assessment — General requirements for bodies operating certification of persons.
61. ISO (2012): ISO/IEC 17065:2012 - Conformity assessment — Requirements for bodies certifying products, processes and services.
62. ISO (2013): ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements.
63. ISO (2013): ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls.
64. ISO (2013): ISO/IEC 27036-3:2013 - Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security.

65. ISO (2013): ISO/IEC TR 20000-5:2013 - Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1.
66. ISO (2014): ISO/IEC 27036-1:2014 - Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts.
67. ISO (2014): ISO/IEC 27036-2:2014 - Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements.
68. ISO (2015): ISO 22317:2015 - Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA).
69. ISO (2015): ISO/IEC 17021-1:2015 - Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements.
70. ISO (2015): ISO/IEC 27033-1:2015 - Information technology — Security techniques — Network security — Part 1: Overview and concepts.
71. ISO (2015): ISO/IEC TR 20000-11:2015 - Information technology — Service management — Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®.
72. ISO (2016): ISO/IEC 24760-3:2016 - Information technology — Security techniques — A framework for identity management — Part 3: Practice.
73. ISO (2016): ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management.
74. ISO (2016): ISO/IEC 27036-4:2016 - Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services.
75. ISO (2017): ISO/IEC 20000-6:2017 - Information technology — Service management — Part 6: Requirements for bodies providing audit and certification of service management systems.
76. ISO (2017): ISO/IEC 27021:2017 - Information technology — Security techniques — Competence requirements for information security management systems professionals.
77. ISO (2018): ISO 19011:2018 - Guidelines for auditing management systems.
78. ISO (2018): ISO 21001:2018 - Educational organizations — Management systems for educational organizations — Requirements with guidance for use.
79. ISO (2018): ISO 22331:2018 - Security and resilience — Business continuity management systems — Guidelines for business continuity strategy.
80. ISO (2018): ISO 29992:2018 - Assessment of outcomes of learning services — Guidance.
81. ISO (2018): ISO 31000:2018 - Risk management – Guidelines.
82. ISO (2018): ISO/IEC 20000-1:2018 - Information technology — Service management — Part 1: Service management system requirements.
83. ISO (2018): ISO/IEC 20000-10:2018 - Information technology — Service management — Part 10: Concepts and vocabulary.
84. ISO (2018): ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management.
85. ISO (2018): ISO/IEC 29147:2018 - Information technology — Security techniques — Vulnerability disclosure.
86. ISO (2019): ISO 22301:2019 - Security and Resilience — Business continuity management systems — Requirements.
87. ISO (2019): ISO/IEC 20000-2:2019 - Information technology — Service management — Part 2: Guidance on the application of service management systems.
88. ISO (2019): ISO/IEC 20000-3:2019 - Information technology — Service management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1.
89. ISO (2019): ISO/IEC 20000-7:2019 - Information technology — Service management — Part 7: Guidance on the integration and correlation of ISO/IEC20000-1:2018 to ISO 9001:2015 and ISO/IEC27001:2013.
90. ISO (2019): ISO/IEC 24760-1:2019 - IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts.

91. ISO (2020): ISO 22313:2020 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301.
92. ISO (2020): ISO/IEC 27014:2020 - Information technology — Security techniques — Governance of information security.
93. ISO (2021): ISO 22300:2021 - Security and Resilience - Vocabulary.
94. ISO (2021): ISO 22332:2021 - Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures.
95. ITU-T (2016): X.1038 Security requirements and reference architecture for software-defined networking.
96. LogRythm (2021): Analysis and Detection of Golden SAML Attacks.
97. MITRE (2019): Common Attack Pattern Enumeration and Classification; Retrieved July 16, 2019, from https://capec.mitre.org
98. NIST (2003): SP800-50 - Building an Information Technology Security Awareness and Training Program; Guideline.
99. NIST (2006): SP800-100 - Information Security Handbook: A Guide for Managers. Gaithersburg, MD: NIST.
100. NIST (2006): SP800-92 Guide to Computer Security Log Management.
101. NIST (2017): SP800-190 - Application Container Security.
102. NIST (2018): White Paper - Framework for Improving Critical Infrastructure Cybersecurity.
103. NIST (2019): SP800-204 - Security Strategies for Microservices-based Application Systems.
104. NIST (2020): SP800-181Rev1 Workforce Framework for Cybersecurity (NICE Framework).
105. NIST (2020): White Paper - Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF).
106. NIST (2021): NIST SP-800-53A - Assessing Security and Privacy Controls in Information Systems and Organizations.
107. NIST (2021): SP800-154 Guide to Data-Centric System 3 Threat Modeling.
108. NIST (2021): SP800-204B - Attribute-based Access Control for Microservices-based Applications using a Service Mesh.
109. NIST (2021): SP800-53A Risk Management Framework - Assessing Security and Privacy Controls in Information Systems and Organizations. Guideline.
110. NIST (n.d.): SP800-53 Rev. 5.1 and SP 800-53B; Retrieved from nist.org: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=PE
111. OWASP (2017): owasptopten.org; Retrieved from https://www.owasptopten.org/
112. SANS Institute (2021): Security Policy Templates; Retrieved from https://www.sans.org/information-security-policy/
113. TM Forum (2021): ETOM GB 921 Business Process Framework.
114. W. Bautista Jr (2019): Cyber kill chain and the OODA loop; O'Reilly Editions

ANNEX – TAXONOMY FOR STANDARDS

This section acts as a reminder of the definitions of document typologies from the EU regulatory framework and the ISO.

A.1 DOCUMENT TYPOLOGIES DEFINED BY THE EU REGULATION

The European Union’s Regulation (EU) No 1025/2012, 2012 stipulates the following provisions:

A **Technical specification** is a document that prescribes technical requirements to be fulfilled by a product, process, service or system (..).

Depending on the source of such specification, it could be a standard (*standard* means a technical specification adopted by a recognised standardisation body for repeated or continuous application) at the international, regional (e.g. European) or national level.

Additionally, there is the *European standardisation deliverable*, which refers to any technical specification other than a European standard adopted by a European standardisation organisation for repeated or continuous application.

Technical specifications, not being standards nor European standardisation deliverables, could be identified as equivalent to standards if they meet the requirements set up in Annex II of Regulation 1025/2012.

If the taxonomy based on EU Regulation 1025/2012 were considered it could look like:

A. Technical specification – document containing the requirements for:
A1 – Technical specification – standard
A2 – Technical specification – European standardisation deliverable considered as a standard (adopted by one of the European Standards Organisations)
A3 – Technical Specification – standard (according to the rules and principles set up in Annex II of the Regulation)
B. Document that contains information other than requirements:
B1 – (Name of a Recognised Standardisation Body) standard – Framework
B2 – (Name of a Recognised Standardisation Body) standard – Guidelines
B3 – (Name of a Recognised Standardisation Body) standard – Best practices
B4 – (Name of a Recognised Standardisation Body) standard – Vocabulary

A.2 DOCUMENT TYPOLOGIES DEFINED BY ISO

If we consider the ISO taxonomy we are dealing with the following (according to ISO):

Standard: is a document established by consensus and approved by a recognised body that provides for common and repeated use rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

International Standard: is a standard that is adopted by an international standardising or standards organisation and made available to the public.

Technical Specification (TS): is a document published by ISO or IEC for which there is, in the future, the possibility of agreement on an International Standard but for which at present:

- the required support for approval as an International Standard cannot be obtained,
- there is doubt on whether consensus has been achieved,
- the subject matter is still under technical development, or
- there is another reason precluding immediate publication as an International Standard.

Technical Report (TR): is a document published by ISO or IEC containing collected data of a different kind from that normally published by ISO or IEC.

If the ISO taxonomy were considered it could look like:

A. Standards
A1 – (Name of a Recognised Standardisation Body) Standard – Requirements
A2 – (Name of a Recognised Standardisation Body) Standard – Framework
A3 – (Name of a Recognised Standardisation Body) Standard – Guidelines
A4 – (Name of a Recognised Standardisation Body) Standard – Vocabulary
B. Technical reports
B1 – ISO Technical Report – Guidelines
B2 – ISO Technical Report – Best practices
C. Non-standard documents
C1 – (Name of the Issuer) – Guidelines
C2 – (Name of the Issuer) – Best Practices

ANNEX – MAPPING

In the detailed analysis, to keep the information in the table manageable, the convention used in this annex is proposed to refer to one or several stakeholders, one or several documents, under a common label.

A.3 REFERENCING THE 5G TECHNICAL AND FUNCTIONAL DOMAINS

In the detailed analysis, to keep the information in the table manageable, a convention specific to this document is proposed to refer to one or several 5G technical and functional domains under a common label. The table below provides for every 5G domain, the associated label.

5G Technical and functional domains	Definition
5G Use cases	End-to-end services based on 5G, characterised by how they use and/or transmit data. Example: 'Vehicle-to-everything', eMBB, mMTC, URLLC.
Multi Access Edge Computing (MEC) Services	Multi access computing services used to bring computation and connectivity closer to the end-user in order to meet the requirements for data transmission speed and latency.
Physical Infrastructure	Set of premises including hardware and software for computation, storage and transmission as well as the related technical environment (energy, air conditioning, cable paths, civil works infrastructures, etc.).
Virtualised Infrastructure	Computing, storage and networking capacities on demand.
Radio Access Network (RAN)	Logical and hardware components making up the functions of the radio access network. It includes mainly distribution units and control units for radio access.
Multi Access Edge Computing (MEC) Infrastructure	Infrastructure related to the decentralisation of cloud functions (storage of data and computing) located closer to the user or edge device.
5G Core Network, Network Function (CN NF)	Central part of the 5G infrastructure which enables new functions related to multi-access technologies. Its main purpose is to deliver services over all kinds of networks (wireless, fixed, converged).
Data Network (DN)	Connectivity to external data, content, services and other resources available outside the 5G network. The data network is also used to interconnect different 5G networks, operators and providers.
Transport	Part of the network ensuring the connectivity between the access and core networks.
Management and Orchestration (MANO)	Software, operations tools and the related environment used to automate operations that relate to the lifecycle of the infrastructure and service components.

A.4 REFERENCING THE STAKEHOLDERS

In the detailed analysis, to keep the information in the table manageable, a convention specific to this document is proposed to refer to one or several stakeholders under a common label. The table below provides for every stakeholder category, the list of the concerned stakeholders is represented by the designation provided in Section 2.1.3 *5G Stakeholders.*

Stakeholder category	Definition
5G Service customer or consumer	Entities that use services that are offered by a service provider (SP). In the context of 5G, these would be, for example, vertical industries and their private networks. In addition, consumers of 5G services without a business relation with a 5G service provider (e.g. end users) are included in this category. **This category may implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services.**
Telecommunications sector (Telecom)	This category encompasses entities that are responsible for the manufacture, deployment and operation of 5G networks, such as: • Mobile network operators: entities providing mobile network services to users, operating their own network, if necessary with the help of third parties. • Suppliers of mobile networks: entities providing services or infrastructure to MNOs in order to build and/or operate their networks (both telecom equipment manufacturers and other third-party suppliers, such as cloud infrastructure providers and network infrastructure providers and managed services providers). • Service provider (SP): entities that design, build and operate services using aggregated network services such as, for example, communication service providers offering traditional telecom services, digital service providers offering digital services such as enhanced mobile broadband and IoT to various vertical industries, or network slice as a service (NSaaS) providers offering a network slice along with the services that it may support and configure. • Virtualisation infrastructure service providers (VISP): entities that provide virtualised infrastructure services and that design, build and operate virtualisation infrastructure(s). The infrastructure comprises networking (e.g. for mobile transport) and computing resources (e.g. from computing platforms). **This category may implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services.**
Datacentre services providers (DCSP)	Entities that provide data centre services and that design, build and operate their data centres. A DCSP differs from a VISP by offering 'raw' resources (i.e. host servers) in rather centralised locations and simple services for consumption of these raw resources. A VISP rather offers access to a variety of resources by aggregating multiple technology domains and making them accessible through a single API. **This category may implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services.**
Connected devices industry	This category includes manufacturers of connected devices and related service providers, meaning entities providing objects or services that will connect to 5G networks (e.g. smartphones, connected vehicles, e-health) and related service components hosted in a 5G control plane as defined in service-based architecture or mobile edge computing. **This category may implement standards, specifications and guidelines to achieve the security objectives for the safe use, deployment and operation of 5G networks and/or services.**

Cybersecurity assessment	This category includes entities that assess the security of 5G networks and systems e.g. auditing companies and accredited 5G laboratories. **This category audits the implementation of standards, specifications and guidelines.**
Cybersecurity information exchange	This category includes entities that share threat intelligence and incident-related information, for example information sharing and analysis centres (ISACs) and cyber security incident response team (CSIRTs). **This category may implement standards, specifications and guidelines to securely exchange cyber-intelligence.**
Standards development organisations (SDOs), associations, alliances	**This category encompasses entities that develop and promote the adoption of standards, specifications and guidelines**, for example GSMA and 3GPP.
Research and innovation organisations	This category encompasses entities contributing to R&D and innovation tasks related to all kinds of innovative actions in the areas related to 5G, including verticals. It also includes open source organisations or communities providing technological support and guidance in the development of 5G functions and services, as well as public-private partnerships and innovation programmes. **This category exposes gaps in standardisation and creates innovations that can lead to advancements in standardisation, by acting as starting points for new standards, specifications and guidelines.**

A.5 REFERENCING THE EXISTING LITERATURE

In the detailed analysis, to keep the information in the detailed analysis table manageable, a convention specific to this document is proposed for referring to one or several documents under a common cluster for easy reference.

The clustering choice is based on either the family of documents or common security theme. The table below provides for every group, the reference shorthand, the descriptive title, the list of concerned documents based on Section *6 Bibliography*, and the document taxonomy from Section *2.2*.

Reference shorthand **Descriptive title**	**References from the bibliography**	**Document taxonomy**
ISOIEC27K **A selection of ISO/IEC JTC1 SC27 requirements and code of practice to setup information security processes.**	(ISO, ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements, 2013) (ISO, ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls, 2013) (ISO, ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management, 2018) (ISO, ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management, 2016)	Standard
ISOIEC20K **A selection of ISO/IEC processes mapped for service delivery.**	(ISO, ISO/IEC 20000-1:2018 - Information technology — Service management — Part 1: Service management system requirements, 2018) (ISO, ISO/IEC 20000-2:2019 - Information technology — Service management — Part 2: Guidance on the application of service management systems, 2019) (ISO, ISO/IEC 20000-3:2019 - Information technology — Service management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1, 2019) (ISO, ISO/IEC TR 20000-5:2013 - Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1, 2013) (ISO, ISO/IEC 20000-6:2017 - Information technology — Service management — Part 6: Requirements for bodies providing audit and certification of service management systems, 2017) (ISO, ISO/IEC 20000-7:2019 - Information technology — Service management — Part 7: Guidance onthe integration and correlation of ISO/IEC20000-1:2018 to ISO 9001:2015 and ISO/IEC27001:2013 , 2019) (ISO, ISO/IEC 20000-10:2018 - Information technology — Service management — Part 10: Concepts and vocabulary, 2018) (ISO, ISO/IEC TR 20000-11:2015 - Information technology — Service management — Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®, 2015)	Standard

	(TMForum, 2021) (IETF, 2004) (ISO, ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls, 2013): 12.1 Operational procedures and responsibilities	
SUPPLSEC **A selection of references for the security of suppliers.**	(ISO, ISO/IEC 27036-1:2014 - Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts, 2014) (ISO, ISO/IEC 27036-2:2014 - Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements, 2014) (ISO, ISO/IEC 27036-3:2013 - Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security, 2013) (ISO, ISO/IEC 27036-4:2016 - Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services, 2016) (GSMA, GSMA FS.16 - NESAS Development and Lifecycle Security Requirements v2.0, 2021)	Standard
POLTEMPLATES **A selection of guidelines to build security policies**	(SANS Institute, 2021)	Guideline
RM **A selection of references for cybersecurity risk management and related assessments**	(ISO, ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management, 2018) (ENISA, Methodology for Sectoral Cybersecurity Assessments, 2021) (Cloud Security Alliance, 2015) (TMForum, 2021) *Note: The eTOM consists in a process map reference framework. It's a useful reference for identifying business processes. However, the eTOM material does not provide any coverage on the implementation of security measures other than their use to identify a scope of governance for S01 and a scope of primary assets for SO2.* (ISO, ISO 31000:2018 - Risk management – Guidelines, 2018)	Standard
	(ANSSI, EBIOS Risk Manager, 2018)**,**	Guideline

	(MITRE, Common Attack Pattern Enumeration and Classification, 2019), (NIST, SP800-53A Risk Management Framework - Assessing Security and Privacy Controls in Information Systems and Organizations, 2021), (EBIOS, 2021) (CIS, CIS Risk Assessment Method, 2018) (Informationstechnik, 2017)	
ENISATL **A selection of references for ENISA works related to threats**	(ENISA, ENISA Threat Landscape for 5G Networks Updated, 2020) (ENISA, Threat Landscape for 5G Networks, 2019) (ENISA, EU Coordinated Risk Assessment of 5G Networks Security, 2019)	Report
SP800HR **A selection of references for security related to human resources**	(NIST, SP800-50 - Building an Information Technology Security Awareness and Training Program, 2003) (NIST, SP800-100 - Information Security Handbook: A Guide for Managers, 2006) (NIST, SP800-181Rev1 Workforce Framework for Cybersecurity (NICE Framework), 2020) (ISO, ISO 29992:2018 - Assessment of outcomes of learning services — Guidance, 2018) (ISO, ISO/IEC 27021:2017 - Information technology — Security techniques — Competence requirements for information security management systems professionals, 2017) (ISO, ISO/IEC 17024:2012 - Conformity assessment — General requirements for bodies operating certification of persons, 2012) (ISO, ISO 21001:2018 - Educational organizations — Management systems for educational organizations — Requirements with guidance for use, 2018)	Guideline
IAM **A selection of references for identity and access management**	(ISO, ISO/IEC 24760-1:2019 - IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts, 2019) (ISO, ISO/IEC 24760-3:2016 - Information technology — Security techniques — A framework for identity management — Part 3: Practice, 2016) (NIST, SP800-204B - Attribute-based Access Control for Microservices-based Applications using a Service Mesh, 2021)	Standard

	(ETSI, ETSI GS NFV-SEC 003 - Network Functions Virtualisation (NFV) - NFV Security - Security and Trust Guidance, 2014) (ETSI, ETSI GS NFV-SEC 014 - Network Functions Virtualisation (NFV) Release 3 - NFV Security - Security Specification for MANO Components and, 2018) (IETF, 2004) (ISO, ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements, 2013): 12.1 Operational procedures and responsibilities	
DEVSECOPS **A selection of references for security in the IT lifecycle**	(NIST, SP800-204 - Security Strategies for Microservices-based Application Systems, 2019) (NIST, SP800-190 - Application Container Security, 2017) (NIST, White Paper - Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF), 2020) (ISO, ISO/IEC/IEEE 29119-1:2013 Software and systems engineering — Software testing — Part 1: Concepts and definitions, 2013)	Guideline
3GPP-All **3GPP Technical specifications from the library**	The whole of the 3GPP list from the bibliography. Note : 3GPP technical specifications have been considered as technical features that are part of the capabilities of the network. 3GPP Technical specifications have been considered as addressing a security measure only when they have been deemed valid as a stand-alone input to a given security measure.	Specification
NFVSEC **A selection of references for the security of network functions virtualisation**	(ISO, ISO/IEC 27033-1:2015 - Information technology — Security techniques — Network security — Part 1: Overview and concepts, 2015) (ETSI, Network Function Virtualisation (NFV);Reliability; Report on the resilience of NFV-MANO critical capabilities, 2017) (ETSI, Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification, 2017) (ETSI, Network Functions Virtualisation (NFV);Architectural Framework, 2014)	Specification

eUICC **A selection of references for security in the eUICC domain**	(GSMA, PRD FS.04 GSMA SAS Standard for UICC Production) (GSMA, PRD FS.05 GSMA SAS Methodology for UICC Production) (GSMA, PRD FS.08 GSMA SAS Standard for Subscription Manager Roles) (GSMA, PRD FS.09 GSMA SAS Methodology for Subscription Manager Roles) (GSMA, PRD FS.18 GSMA SAS Consolidated Security Guidelines) (GSMA, PRD SGP.01 Embedded SIM Remote Provisioning Architecture) (GSMA, PRD SGP.02 Remote Provisioning Architecture for Embedded UICC) (GSMA, PRD SGP.21 Remote SIM Provisioning (RSP) Architecture) (GSMA, PRD SGP.22 Remote SIM Provisioning (RSP) Technical Specification)	Specification
CRYPTOTECH **A selection of references for the use of cryptographic techniques**	(3GPP, 3GPP 33.501 Security architecture and procedures for 5G System) (3GPP, 3GPP 33.310 Network Domain Security (NDS); Authentication Framework (AF)) (3GPP, 3GPP 33.210 Network Domain Security (NDS); IP network layer security) (3GPP, 3GPP 33.163 Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST)) (ISO, ISO/IEC 11770-1:2010 - Information technology — Security techniques — Key management — Part 1: Framework, 2010) (ETSI, ETSI GS NFV-SEC 012 - Network Functions Virtualisation (NFV)Release 3; Security; System architecture specification for execution of sensitive NFV components, 2017) (ITU-T, 2016)	Specification
	NIST, 2021, Planning for a Zero Trust Architecture: A Starting Guide for Administrators	Guideline

PHYSEC **A selection of references for physical and environmental security**	(NIST, SP800-53 Rev. 5.1 and SP 800-53B) (ASIS, 2021) (Informationstechnik, 2017) (ISO, ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls, 2013)- 11.1 Secure areas and 11.2 Equipment (ANSI, 2019)	Guideline
HARDEN **A selection of references for technical robustness**	(CIS, CIS Controls® v8, 2021) (OWASP, 2017)	Guideline
VULN **A selection of references for the management of vulnerabilities**	(GSMA, GSMA FS.23 - Coordinated Vulnerability Disclosure, 2020) (ISO, ISO/IEC 29147:2018 - Information technology — Security techniques — Vulnerability disclosure, 2018) (ISO, ISO/IEC 17960:2015 Information technology — Programming languages, their environments and system software interfaces — Code signing for source code, 2015) (ISO, ISO/IEC 30111:2019 - Information technology — Security techniques — Vulnerability handling processes, 2019) (ISO, ISO/IEC TS 30104:2015 - Information Technology — Security Techniques — Physical Security Attacks, Mitigation Techniques and Security Requirements, 2015)	Guideline Standard
THREATMOD **A selection of references for threat modelling and security monitoring, including threat intelligence capabilities**	(ENISA, Threat Taxonomy, 2016) (MITRE, Common Attack Pattern Enumeration and Classification, 2019) (NIST, SP800-92 Guide to Computer Security Log Management, 2006) (NIST, SP800-154 Guide to Data-Centric System 3 Threat Modeling, 2021) (CSIAC, 2021) (Carder, How to build a SOC with limited resources, 2020)	Guideline

	(Carder, Security Operation Centers Maturity Model, 2020) (LogRythm, 2021) (W. Bautista Jr, 2019) (NSA & CISA, 2021) (ISO, ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls, 2013): 6.1.4 Contact with special interest groups and 12.4 Logging and monitoring, (GSMA, GSMA FS.11 - SS7 Interconnect Security Monitoring and Firewall Guidelines, 2019) (GSMA, GSMA FS.19 - Diameter Interconnect Security, 2019) (GSMA, GSMA FS.37 - GPRS Tunnelling Protocol User Security, 2020)	
SECASSUR **A selection of references for security assurance and related guidelines**	The GSMA Network Equipment Security Assurance Scheme documents: Same as 3GPP Technical Specifications: 33.166, 33.117, 33.216, 33.250, 33.511, 33.512, 33.517, 33.518, 33.519 However, the following GSMA Technical Specifications are contributing: (GSMA, TS 33.513 - 5G Security Assurance Specification (SCAS); User Plane Function (UPF)) (3GPP, TS 33.514 - 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class) (GSMA, TS 33.515 - 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class)	Specification
AUDIT **A selection of references for audit planning and assessment**	(ISO, ISO/IEC 27014:2020 - Information technology — Security techniques — Governance of information security, 2020) (ISO, ISO 19011:2018 - Guidelines for auditing management systems, 2018) (NIST, NIST SP-800-53A - Assessing Security and Privacy Controls in Information Systems and Organizations, 2021) (ISO, ISO/IEC 17021-1:2015 - Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements, 2015) (ISO, ISO/IEC 17065:2012 - Conformity assessment — Requirements for bodies certifying products, processes and services, 2012)	Standard
BCM **A selection of references for planning and implementing**	(TMForum, 2021) (ISO, ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls, 2013) - 12.3 Backup and 17 Information security aspects of business continuity management	Standard

organisational and technical resilience	Business continuity and crisis management standards (ENISA, Report on Cyber Crisis Cooperation and Management, 2014) (ISO, ISO 22300:2021 - Security and Resilience - Vocabulary, 2021) (ISO, ISO 22301:2019 - Security and Resilience — Business continuity management systems — Requirements, 2019) (ISO, ISO 22313:2020 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301, 2020) (ISO, ISO 22317:2015 - Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA), 2015) (ISO, ISO 22331:2018 - Security and resilience — Business continuity management systems — Guidelines for business continuity strategy, 2018) (ISO, ISO 22332:2021 - Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures, 2021)	
	NIST SP800-160 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (NIST, White Paper - Framework for Improving Critical Infrastructure Cybersecurity, 2018)	Guideline

A.6 DETAILED MAPPING

This section provides the detailed analysis of standardisation coverage derived from the 5G domains and lifecycle.

The columns of this table are explained hereunder:

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
List of the 5G security measures per security domain and objectives as defined in Section 2.1.4 *5G Security domains, objectives and measures.* The detailed mapping distinguishes general security measures and 5G-specific ones.	The taxonomy of the reference documents. This column is intended to keep the reader aware of what the literature group is about. A *standard* and a *specification* tend to express 'What to do' or 'Security features', whereas a *guideline* tends to provide elements on the 'How to implement security', closer to considerations of the build and the run. This is described in Section *2.2 Taxonomy of Documents Considered*	A group name to designate several literature references identified as matching (but not necessary fulfilling) the purpose of the security measure. The group names are described in Annex *6.A.5 referencing the existing literature*	A group name designating stakeholders of the 5G ecosystem covered by the literature identified. The group names are described in Annex *6.A.4 referencing the stakeholders*	A group name referring to the 5G domains covered by the literature identified. The 5G domains are grouped according to Annex *6.A.3 referencing the 5G technical and functional domains*	Lifecycle processes covered by the literature identified. The lifecycle processes are provided in Section *2.1.2 Technology lifecycle processes.*

The conventions for the comments used in the detailed analysis are as follows.

'All': the reference document is considered applicable to every entity in the ecosystem, at various degrees and at different depths. The specific degree or depth of applicability to each entity are not assessed here.

'Not put into context and not immediately actionable' means that the reference document is generic and may be applied to the entity. Further work is required to tailor it to the specific context.

The coverage of the references has been assessed by considering how they can be used to serve given security measures. When the reference only mentions the security measure without providing a specific relevant tool for its implementation, the reference is not mentioned.

D1 - GOVERNANCE AND RISK MANAGEMENT

SO 1 - Information security policy

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Set a high-level security policy addressing the security of networks and services. Make key personnel aware of the security policy.	Standard Guideline	ISOIEC27K RM	All except opensource community	All (high level) IT Security detailed but not put in 5G context	All (high level)
Set detailed information security policies for critical assets and business processes. Make all personnel aware of the security policy and what it implies for their work. Review the security policy following incidents.	Standard Guideline	ISOIEC27K SP800HR	All except opensource community	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Review the information security policies periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	Standard	ISOIEC27K	All except opensource community	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)

SO 2 - Governance and risk management

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Make a list of the main risks for security of networks and services, taking into account the main threats for critical assets. Make key personnel aware of the main risks and how they are mitigated.	Standard Guideline Report	ISOIEC27K RM, ENISATL SP800HR	All except opensource community	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Set up a risk management methodology and/or tools based on industry standards. Ensure that key personnel use the risk management methodology and tools. Review the risk assessments following changes or incidents. Ensure residual risks are accepted by management.	Standard Guideline Report	ISOIEC27K RM ENISATL SP800HR	All except opensource community	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents.	Standard Guideline Report	ISOIEC27K RM ENISATL	All except opensource community	All	All

5G specific check	Applicable documents taxonomy	Reference to the documents	Coverage of Stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Is the list of identified risks aligned with the main risks for 5G networks identified in the Coordinated risk assessment?	Guideline Report	RM ENISATL	All except opensource community	All	All
Are threats related to the exposure to potentially high-risk suppliers or managed service providers, including those residing in other jurisdictions, taken in consideration?	Guideline Standard	RM ISOIECSUPL	Telecom	Need to be implemented according to Member States' provisions	Build and Run
Has a potential dependency on a single supplier of 5G equipment been considered when assessing the main risks for security of networks and services?	Guideline Standard	RM ISOIECSUPL	All except opensource community	All	Build and Run

SO 3 - Security roles and responsibilities

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G domains	Coverage of lifecycle processes
Assign security roles and responsibilities to personnel. Make sure the security roles are reachable in case of security incidents.	Standard Guideline	ISOIEC27K SP800HR	Telecom and DCSP	All	All
Personnel is formally appointed in security roles. Make personnel aware of the security roles in your organisation and when they should be contacted.	Guideline	SP800HR	All	All	All
Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.	Guideline	SP800HR	All	All	All

SO 4 - Security of third-party dependencies

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Include security requirements in contracts with third-parties, including confidentiality and secure transfer of information.	Standard	ISOIEC27K SUPPLSEC	SC, Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Set a security policy for contracts with third-parties. Ensure that all procurement of services/products from third-parties follows the policy. Review security policy for third parties, following incidents or changes. Demand specific security standards in third-party supplier's processes during procurement. Mitigate residual risks that are not addressed by the third party.	Standard	ISOIEC27K SUPPLSEC	SC, Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Keep track of security incidents related to or caused by third-parties. Periodically review and update security policy for third parties at regular intervals, taking into account past incidents, changes, etc.	Standard	ISOIEC27K SUPPLSEC	SC, Telecom and DCSP	All (but not put into context and not immediately actionable)	Run

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Does the MNO have security requirements placed on third parties as part of contractual arrangements and is there a mechanism to monitor that suppliers are meeting said contractual arrangements?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Does the MNO require suppliers to comply with relevant EU certification schemes for 5G network components, customer equipment and/or suppliers' processes or for other non 5G-specific ICT products and services, such as end-user devices and/or cloud services?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Does the MNO require suppliers to demonstrate the quality level of internal information security processes, including having security by design built in the product development process?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Does the MNO require suppliers to adhere to best practices and industry standards throughout the lifetime of the product?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Does the MNO require suppliers to provide support for periodic security and penetration testing of its products?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Does the MNO require suppliers to guarantee there are no intentionally introduced vulnerabilities in their products and to disclose and patch any known vulnerabilities in their products without undue delay?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Does the MNO require suppliers to have implemented the security requirements of relevant 5G technical specifications and industry standards by default?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Does the MNO require suppliers to guarantee adequate protection and non-disclosure of confidential information from or about its customers to third parties, in particular to foreign intelligence or security authorities?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run
Does the MNO require its suppliers to support the MNO in investigating and remedying security incidents?	Standard	ISOIEC27K SUPPLSEC	Telecom and DCSP	All (but not put into context and not immediately actionable)	Build and Run

D2 - HUMAN RESOURCES SECURITY

SO 5 - Background checks

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Check professional references of key personnel (system administrators, security officers, guards, etc.).	Standard Guideline	ISOIEC27K SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Perform background checks/screening for key personnel, when needed and legally permitted. Set up a policy and procedure for background checks.	Standard Guideline	ISOIEC27K SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents.	Standard Guideline	ISOIEC27K SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Does the list of personnel for whom background checks or screening have been performed also include contractors and third-party suppliers?	Standard Guideline	ISOIEC27K SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Are personnel who will have access (either physically or through management systems) to critical or sensitive components of 5G networks security-vetted (as stipulated in the provisions of the Toolbox technical measure TM06)?	Standard Guideline	ISOIEC27K IAM SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All

SO 6 - Security knowledge and training

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Provide key personnel with relevant training and material on security issues.	Standard Guideline	ISOIEC27K SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge. Organise trainings and awareness sessions for personnel on security topics important for your organisation.	Standard Guideline	ISOIEC27K SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Review and update the training programme periodically, taking into account changes and past incidents. Test the security knowledge of personnel.	Standard Guideline	ISOIEC27K SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Has the training programme been updated to include coverage of specialised 5G technical topics?	Guideline	SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Is there an evidence that the key personnel who will be in charge of deploying and operating 5G networks have followed the updated training courses?	Guideline	SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Is there an evidence that the personnel who will have access (either physically or through management systems) to critical or sensitive network components are trained and qualified (as stipulated in the provisions of the Toolbox technical measure TM06)?	Guideline Standard	SP800HR IAM	Telecom and DCSP	All (but not put into context and not immediately actionable)	All

SO 7 - Personnel changes

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Following changes in personnel revoke access rights, badges, equipment etc., if no longer necessary or permitted. Brief and educate new personnel on the policies and procedures in place.	Standard Guideline	ISOIEC27K IAM SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Implement policy/procedures for personnel changes, taking into account timely revocation of access rights, badges and equipment. Implement policy/procedures for education and training for personnel in new roles.	Standard Guideline	ISOIEC27K IAM SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All
Periodically check that the policy/procedures are effective. Review and evaluate policy/procedures for personnel changes, taking into account changes or past incidents.	Standard Guideline	ISOIEC27K IAM SP800HR	Telecom and DCSP	All (but not put into context and not immediately actionable)	All

SO 8 - Handling violations

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Hold personnel accountable for security incidents caused by violations of policies, for example via the employment contract.	Standard Guideline	ISOIEC27K SP800HR	All	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Set up procedures for violations of policies by personnel.	Standard Guideline	ISOIEC27K SP800HR	All	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Periodically review and update the disciplinary process, based on changes and past incidents.	Standard Guideline	ISOIEC27K SP800HR	All	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)

D3 - SECURITY OF SYSTEMS AND FACILITIES

SO 9 - Physical and environmental security

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Prevent unauthorised physical access to facilities and set up adequate environmental controls, to protect provider assets against unauthorised access, burglary, fire, flooding, etc	Guideline	PHYSEC	SC, Telecom and DCSP	All except anything outside a datacentre facility	Run
Implement a policy for physical security measures and environmental controls. Industry standard implementation of physical and environmental controls. Apply reinforced controls for physical access to critical assets.	Guideline	PHYSEC	SC, Telecom and DCSP	All except anything outside a datacentre facility	Run
Evaluate the effectiveness of physical and environmental controls periodically. Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents.	Guideline	PHYSEC	SC, Telecom and DCSP	All except anything outside a datacentre facility	Run

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Are there documented, additional, risk-based controls for physical security for MEC and base stations included in the policy for physical security measures?	Guideline	PHYSEC	SC, Telecom and DCSP	MEC	All
Are there documented additional, adequate physical infrastructure controls (for example perimeter security for infrastructure and administrative premises, alarms and CCTV for detecting and recording incidents), especially for equipment locations which are unmanned, in place?	Guideline	PHYSEC	SC, Telecom and DCSP	Physical infrastructure	All
Are there any controls in place to allow failsafe remote shutdown (or data clearing) for stolen equipment and/or to require re-authentication or configuration after a physical attack or power failure at base stations?	Guideline	PHYSEC	SC, Telecom and DCSP	Physical infrastructure	All

Is there evidence that access controls are in place for individuals accessing premises, including assurance that they are security-vetted, trained and qualified and that any access, especially by third parties and contractors, is strictly monitored?	Guideline Standard	PHYSEC IAM	SC, Telecom and DCSP	Physical infrastructure	All
Do physical security controls included in the policy for physical security measures cover (multi-vendor) spare part management, at least for critical assets?	Guideline	PHYSEC	SC, Telecom and DCSP	Physical infrastructure	All

SO 10 - Security of supplies

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Ensure security of critical supplies.	Standard Guideline	ISOIEC27K PHYSEC	SC, Telecom and DCSP	Physical infrastructure	All
Implement a policy for security of critical supplies. Implement industry standard security measures to protect critical supplies and supporting facilities (e.g. passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.).	Standard Guideline	ISOIEC27K PHYSEC	SC, Telecom and DCSP	Physical infrastructure	All
Implement state-of-the-art security measures to protect critical supplies (such as active cooling, UP, hot standby power generators, SLAs with fuel delivery companies, redundant cooling and power backup systems). Review and update policy and procedures to secure critical supplies regularly, taking into account changes and past incidents.	Standard Guideline	ISOIEC27K PHYSEC	SC, Telecom and DCSP	Physical infrastructure	All

SO 11 – Access control to network and information systems

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Users and systems have unique IDs and are authenticated before accessing services or systems. Implement logical access control mechanism for network and information systems to allow only authorised use.	Specification	3GPP IAM	SC, Telecom and DCSP	All	Think, Build
Implement policy for protecting access to network and information systems, addressing, for example, roles, rights, responsibilities and procedures for assigning and revoking access rights. Choose appropriate authentication mechanisms, depending on the type of access. Monitor access to network and information systems, have a process for approving exceptions and registering access violations. Reinforce controls for remote access to critical assets of network and information systems by third parties.	Standard Guideline	ISOIEC27K IAM 3GPP	SC, Telecom and DCSP	All	Think, Build, Run
Evaluate the effectiveness of access control policies and procedures, and implement cross checks on access control mechanisms. Access control policy and access control mechanisms are reviewed and, when needed, revised.	Standard Guideline	ISOIEC27K IAM SECASSUR	SC, Telecom and DCSP	All	All

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Are there any additional strict network access controls applied according to the updated risk assessment that particularly considers 5G network architecture elements?	Standard Specification	ISOIEC27K IAM 3GPP 33.501; 33.517; 33.518; 33.519	SC, Telecom and DCSP	All	All
Is there an evidence demonstrating how the principle of least privilege is applied (including the explanation on how various rights in the network, such as access rights between network functions, network administrators' rights and alike are minimised)?	Standard	ISOIEC27K IAM	SC, Telecom and DCSP	All	All
Is there an evidence showing how the principle of segregation of duties is applied?	Standard	ISOIEC27K IAM	SC, Telecom and DCSP	All	All

Is there an evidence that the access control policy has been reviewed and revised in the context of assessment of 5G risks?	Standard	ISOIEC27K IAM	SC, Telecom and DCSP	All	All
Does the (revised) access control policy include provisions for restricting and/or strict controlling of remote access by third parties, especially by suppliers or managed service providers considered to be high-risk or accessing the network from outside of EU?	Standard	ISOIEC27K IAM	SC, Telecom and DCSP	All	All
Do authentication mechanisms implemented follow general good practices and industry standards for strong authentication?	Standard	ISOIEC27K IAM	SC, Telecom and DCSP	All	All
Are there controls in place to only allow temporary access to third parties and/or remote access and that no permanent credentials are granted (e.g. temporary or one-time passwords, usable only for designated tasks)?	Standard	ISOIEC27K IAM	SC, Telecom and DCSP	All	All
Is there a centralised solution for Privileged Access Management (PAM) in place1?	Standard	ISOIEC27K IAM	SC, Telecom and DCSP	All	All

SO 12 - Integrity of network and information systems

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Make sure that the software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls. Check for malware on (internal) network and information systems.	Guideline	RM	SC, Telecom and DCSP	All	Build, Run
Implement industry standard security measures, providing defence-in-depth against the tampering and altering of systems. Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks.	Guideline	RM	SC, Telecom and DCSP	All	All
Set up state-of-the-art controls to protect the integrity of systems. Evaluate and review the effectiveness of measures to protect the integrity of systems.	Guideline	RM	SC, Telecom and DCSP	All	All

5G specific check	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Do software patching procedures follow industry standard best practices for ensuring that software products or components have not been altered (e.g. appropriate cryptographic methods for integrity and authenticity protection)?	Standard	VULN	SC, Telecom and DCSP	All	RUN
Are there documented and tested processes for delivery and implementation of security patches to vulnerable components?	Standard	VULN	SC, Telecom and DCSP	All	RUN
Are there appropriate physical protection mechanisms in place to ensure that hardware products have not been tampered with (e.g. physical security protection for equipment transport)?	Standard	VULN	SC, Telecom and DCSP	All	RUN
Are there specific timeframes for applying security patches to vulnerable components, particularly in the case of high and critical vulnerabilities?	Standard	VULN	SC, Telecom and DCSP	All	RUN

SO 13 - Use of encryption

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage and/or transmission via networks.	Standard Specification	ISOIEC27K 3GPP33210 3GPP33501	SC, Telecom and DCSP	All	All
Implement encryption policy. Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys.	Specification	3GPP 3GPP33210 3GPP33501 CRYPTOTECH	SC, Telecom and DCSP	All	Think and Build
Review and update the encryption policy. Use state-of-the-art encryption algorithms.	Specification	3GPP CRYPTOTECH	SC, Telecom and DCSP	All	Build Run should include lifecycle of certificates

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Is encryption applied for the concealment and protection of customer security critical data, in particular the permanent user identifiers?	Specification	3GPP33501	SC, Telecom and DCSP	All	Build Run should include lifecycle of certificates
Is encryption applied for the protection of signalling traffic between operators?	Specification	3GPP	SC, Telecom and DCSP	All	Build Run should include lifecycle of certificates
Is encryption applied for transport protection between network functions?	Specification	3GPP	SC, Telecom and DCSP	All	Build Run should include lifecycle of certificates
Is encryption applied for the protection of the confidentiality of user and signalling data between user equipment and base stations?	Specification	3GPP	SC, Telecom and DCSP	All	Build Run should include lifecycle of certificates

SO14 - Protection of security critical data

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with. Access to private keys is strictly controlled and monitored.	Specification Specification Guideline	3GPP CRYPTOTECH SECASSUR	SC, Telecom and DCSP	All	All
Implement policy for management of cryptographic keys. Implement policy for management of user passwords.	Specification Specification Guideline	3GPP CRYPTOTECH SECASSUR	SC, Telecom and DCSP	All	All
Review and update key management policy. Review and update user password management policy.	Specification Specification Guideline	3GPP CRYPTOTECH SECASSUR	SC, Telecom and DCSP	All	All

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Are there appropriate controls in place, according to best practices, for the protection of cryptographic key material in UICC (or eUICC)?	Specification Guideline	eUICC SECASSUR	Telecom	eUICC	Think

Are appropriate controls in place, according to best practices, for the protection of cryptographic key material for encryption of subscriber permanent identifiers (SUPI)?	Specification	3GPP33501;
		SECASSUR;
		NFVSEC
		SCP
			Telecom	RAN	All

Are there appropriate controls in place, according to best practices, for the protection of any other cryptographic key material used to encrypt communication between network elements or between different networks?	Specification	3GPP33501;
		SECASSUR;
		NFVSEC
		SCP
			Telecom	All	All

Are there appropriate controls in place for the protection of VNF private keys to authenticate NF exchanges in the 5G core network?	Specification	NFVSEC	Telecom	All	All
Where cryptographic key material is stored on third party key servers, are appropriate contractual arrangements in place with the server provider to ensure security of this key material?	Specification	NFVSEC	Telecom	All	All

D4 - OPERATIONS MANAGEMENT

SO 15 - Operational procedures

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Set up operational procedures and assign responsibilities for the operation of critical systems.	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Implement a policy for the operation of systems to make sure all critical systems are operated and managed in line with predefined procedures.	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Review and update the policy/procedures for the operation of critical systems, taking into account incidents and/or changes.	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)

SO 16 - Change management

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Follow predefined methods or procedures when making changes to critical systems	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Implement policy/procedures for change management, to make sure that changes of critical systems are always done following a predefined way. Document change management procedures, and record for each change the steps of the followed procedure.	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Review and update change management procedures regularly, taking into account changes and past incidents.	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Are there regular assessments of the potential impact of an intended change prior to major system changes, especially when critical or sensitive network components are about to be updated?	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Is there a mechanism in place to ensure that any major actual change implemented, especially for critical or sensitive network components, is recorded and any irregularities encountered during the change process are investigated and, if incident reporting conditions are met, reported to competent authorities?	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Are changes to a virtualised network environment (e.g. through patching of software defined network components) included in the change management policies and procedures?	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Has the MNO given consideration to moving to software development lifecycle best practices such as Agile, Continuous Integration/Continuous Development (CI/CD), and DevSecOps, given 5G's shift to a software based network?	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)

SO 17 - Asset management

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Identify critical assets and configurations of critical systems.	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Implement policy/procedures for asset management and configuration control.	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)
Review and update the asset management policy regularly, based on changes and past incidents.	Standard	ISOIEC20K	SP, Telecom, DCSP	All (needs an effort to put into context)	All (needs an effort to put into context)

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Is asset criticality assessment aligned with the list of critical assets identified in the Coordinated risk assessment?	Guideline	RM, NFVSEC	SP, Telecom	All	Run
Has the MNO established relevant information repositories/registries containing details about deployed technologies and components and are such registries appropriately maintained (e.g. timely updates upon changes to the network)?	Guideline	RM, NFVSEC	SP, Telecom	All	Run
Are there mechanisms envisaged in the MNO policies/procedures for asset management for conducting regular assessments of their physical assets and for categorisation of their physical network assets (e.g. core network assets, transmission hubs, exchanges, base-stations, interconnection and transport links) based on a risk assessment and according to the assets sensitivity/criticality.	Guideline	RM, NFVSEC	SP, Telecom	All	Run
Have policies/procedures for asset management been updated to reflect the fact that 5G networks will likely be virtualised, with VNFs being instantiated and decommissioned in an automated way and do such updates include sufficient provisions to ensure good understanding of the virtual network, including data flows, trust domains and the location and status	Guideline	RM, NFVSEC	SP, Telecom	All	Run

of the physical hosts on which the virtual network resides?					

D5 INCIDENT MANAGEMENT

SO 18 - Incident management procedures

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Make sure personnel is available and prepared to manage and handle incidents. Keep a record of all major incidents.	Standard	ISOIEC27K ISOIEC20K	SC, Telecom, DSCP	All	Run
Implement policy/procedures for managing incidents.	Standard	ISOIEC27K ISOIEC20K	SC, Telecom, DSCP	All	Run
Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate future occurrence of this type of incident. Evaluate incident management policy/procedures based on past incidents.	Standard	ISOIEC27K ISOIEC20K	SC, Telecom, DSCP	All	Run

SO 19 - Incident detection capability

Security Measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Set up processes or systems for incident detection.	Standard Guideline	ISOIEC27K THREATMOD	SC, Telecom, DSCP	All	Run
Implement industry standard systems and procedures for incident detection. Implement systems and procedures for registering and forwarding incidents timely to the appropriate people.	Standard Guideline	ISOIEC27K THREATMOD	SC, Telecom, DSCP	All	Run
Review systems and processes for incident detection regularly and update them taking into account changes and past incidents. Implement state-of-the-art systems and procedures for incident detections	Standard Guideline	ISOIEC27K THREATMOD	SC, Telecom, DSCP	All	Run

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Are relevant logs related to remote network access regularly reviewed according to predefined procedures?	Standard Guideline	ISOIEC27K THREATMOD	SC, Telecom, DSCP	All	Run
Are there capabilities for anomaly detection in place?	Standard Guideline	ISOIEC27K THREATMOD	SC, Telecom, DSCP	All	Run
Is the monitoring infrastructure implemented according to the recommendation from Toolbox, including whether such monitoring infrastructure is established on premises, ideally inside the country or inside the EU?	Standard Guideline	ISOIEC27K THREATMOD	SC, Telecom, DSCP	All	Run
Does the MNO have adequate resources available to monitor, understand and analyse security-related network activity?	Standard Guideline	ISOIEC27K THREATMOD	SC, Telecom, DSCP	All	Run

SO 20 - Incident reporting and communication

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary.	Standard	ISOIEC27K BCM	SC, Telecom, DSCP	All	Run
Implement policy and procedures for communicating and reporting about incidents.	Standard	ISOIEC27K BCM	SC, Telecom, DSCP	All	Run
Evaluate past communications and reporting about incidents. Review and update the reporting and communication plans, based on changes or past incidents.	Standard	ISOIEC27K BCM	SC, Telecom, DSCP	All	Run

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Does the MNO comply with relevant incident reporting provisions within a given legal framework?	Standard	ISOIEC27K BCM	SC, Telecom, DSCP	All	Run

D6 - BUSINESS CONTINUITY MANAGEMENT

SO 21- Service continuity strategy and contingency plans

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Implement a service continuity strategy for the communications networks and/or services provided.	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Implement contingency plans for critical systems. Monitor activation and execution of contingency plans, registering successful and failed recovery times. Implement contingency plans for dependent and inter-dependent critical sectors and services.	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Review and revise service continuity strategy periodically. Review and revise contingency plans, based on past incidents and changes.	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Are there measures in place to ensure supply-chain resilience (e.g. by ensuring that contingency plans consider scenarios of removal of critical suppliers, understanding the related impact and having appropriate failback strategies in place)?	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Are there any special provisions added to existing contingency plans to cover time-critical applications of 5G services, such as URLLC as to ensure higher network availability for such services?	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Is there a map of critical dependencies that may directly or indirectly impact availability or continuity of 5G network services and if corresponding mitigation measures are defined and documented?	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Is there a map of critical sectors and services directly dependent on the continuity of network and service operations and if criticality of such systems is taken in consideration in contingency plans?	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)

SO 22 - Disaster recovery capabilities

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Prepare for recovery and restoration of services following disasters.	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Implement policy/procedures for deploying disaster recovery capabilities. Implement industry standard disaster recovery capabilities, or be assured they are available from third parties (such as national emergency networks).	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Set up state-of-the-art disaster recovery capabilities to mitigate natural and/major disasters. Review and update disaster recovery capabilities regularly, taking into account changes, past incidents and the results of tests and exercises.	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Are there documented plans in place in case of a disaster affecting the ongoing operation of the MNO's network?	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)

D7 - MONITORING, AUDITING AND TESTING

SO 23 - Monitoring and logging policies

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Implement monitoring and logging of critical systems.	Guideline	THREATMOD	SP, Telecom, DCSP	All (needs to be put into context)	Run
Implement a policy for the logging and monitoring of critical systems. Set up tools for monitoring critical systems. Set up tools to collect and store logs of critical systems.	Guideline	THREATMOD	SP, Telecom, DCSP	All (needs to be put into context)	Run
Set up tools for the automated collection and analysis of monitoring data and logs. Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.	Guideline	THREATMOD	SP, Telecom, DCSP	All (needs to be put into context)	Run

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Are there adequate monitoring capabilities in place in line with recommendations from the Toolbox technical measures TM05, to ensure clear visibility and to implement effective network monitoring of at least the critical or sensitive network components or functions, to detect anomalies and to identify and avoid threats including but not limited to threats to 5G core coming from compromised end-user devices?	Guideline	THREATMOD	SP, Telecom, DCSP	All (needs to be put into context)	Run
Does the monitoring and logging policy also include monitoring of VPN and remote access to the 5G network from remote locations?	Guideline	THREATMOD	SP, Telecom, DCSP	All (needs to be put into context)	Run
Is there monitoring in place for roaming and interconnections (e.g. message monitoring and filtering capabilities to identify and block malformed, prohibited and unauthorised packets, to confirm that interfaces are only accessible to the correct external applications and/or networks and to enable audit logging and delivery of data to SIEM for analysis for relevant threat vectors)?	Guideline	THREATMOD	SP, Telecom, DCSP	All (needs to be put into context)	Run

SO 24 - Exercise contingency plans

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Exercise and test backup and contingency plans to make sure systems and processes work and personnel is prepared for large failures and contingencies.	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Implement a programme for exercising backup and contingency plans regularly, using realistic scenarios covering a range of different scenarios over time. Make sure that the issues and lessons learnt from exercises are addressed by the responsible people and that the relevant processes and systems are updated accordingly.	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)
Review and update the exercise plans, taking into account changes, past incidents and contingencies which were not covered by the exercise programme. Involve suppliers and other third parties in exercises, for example, business partners and customers.	Standard	BCM	SC, Telecom, DCSP	All (but not put into context and not immediately actionable)	All (but not put into context and not immediately actionable)

SO 25 - Network and information systems testing

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Test networks and information systems before using them or connecting them to existing systems.	Standard	DEVSECOPS	SC, Telecom, DCSP	All	BUILD
Implement policy/procedures for testing network and information systems. Implement tools for automated testing.	Standard	DEVSECOPS	SC, Telecom, DCSP	All	BUILD
Review and update the policy/procedures for testing, taking into account changes and past incidents.	Standard	DEVSECOPS ISOIEC27K	SC, Telecom, DCSP	All	BUILD, RUN

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G domains	Coverage of lifecycle processes
Are all patches, especially those to critical or sensitive network components or functions, subjected to security testing in a controlled environment prior to deployment?	Standard	VULN	SC, Telecom, DCSP	All	RUN

SO 26 - Security assessments

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G domains	Coverage of lifecycle processes
Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes.	Standard	DEVSECOPS ISOIEC27K VULN	SC, Telecom, DCSP	All	BUILD, RUN
Implement policy/procedures for security assessments and security testing.	Standard	DEVSECOPS ISOIEC27K VULN	SC, Telecom, DCSP	All	BUILD, RUN
Evaluate the effectiveness of policy/procedures for security assessments and security testing. Review and update policy/procedures for security assessments and security testing, taking into account changes and past incidents.	Standard	DEVSECOPS ISOIEC27K VULN SUPPL	SC, Telecom, DCSP	All	BUILD, RUN

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of Stakeholders	Coverage of 5G domains	Coverage of lifecycle processes
Are security tests, vulnerability assessments/scans and penetration tests done on deployment and subsequently, on a periodic basis, for newly deployed network components, in particular for products supplied by suppliers considered to be high-risk?	Standard	DEVSECOPS ISOIEC27K VULN SUPPL	SC, Telecom, DCSP	All	BUILD, RUN

SO 27 - Compliance monitoring

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G technological and functional domains	Coverage of lifecycle processes
Monitor compliance to standards and legal requirements.	Standard	ISOIEC27K BCM	SC, Telecom, DCSP	All (needs effort to be put into context)	Run
Implement policy/procedures for compliance monitoring and auditing.	Standard	ISOIEC27K BCM	SC, Telecom, DCSP	All (needs effort to be put into context)	Run
Evaluate the policy/procedures for compliance and auditing. Review and update the policy/procedures for compliance and auditing, taking into account changes and past incidents.	Standard	ISOIEC27K BCM	SC, Telecom, DCSP	All (needs effort to be put into context)	Run

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G domains	Coverage of lifecycle processes
Is monitoring of compliance with relevant 5G standards (e.g. 3GPP, ETSI NFV2) included in the compliance monitoring policies and procedures?	Guideline	3GPP ETSINFV	Telecom	All	Run

D8 - THREAT AWARENESS

SO 28 - Threat intelligence

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G domains	Coverage of lifecycle processes
Perform regular threat monitoring.	Guideline	THREATMOD	SC, Telecom, DCSP	All	Run
Implement a threat intelligence programme.	Guideline	THREATMOD	SC, Telecom, DCSP	All	Run
Review and update the threat intelligence programme. Threat intelligence programme makes use of state-of-the-art threat intelligence systems.	Guideline	THREATMOD	SC, Telecom, DCSP	All	Run

Security measure (5G-specific)	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G domains	Coverage of lifecycle processes
Does the threat monitoring and/or threat intelligence programme include a variety of threats of particular significance for 5G networks?	Guideline	THREATMOD	SC, Telecom, DCSP	All	Run
Are relevant and current sources and publications and/or relevant CTI tools and platforms consulted or used systematically?	Guideline	THREATMOD	SC, Telecom, DCSP	All	Run

SO 29 - Informing users about threats

Security measure	Applicable documents taxonomy	Reference to the documents	Coverage of stakeholders	Coverage of 5G domains	Coverage of lifecycle processes
Inform end-users of communication networks and services about particular and significant security threats to a network or service that may affect them.	None	None	None	None	None
Implement policy/procedures for regular update of end-users about security threats to network or service that may affect them.	None	None	None	None	None
Review and update the policy/procedures for regular update of end-users about security threats to the network or service that may affect them.	None	None	None	None	None

Security measure (5G-specific)	**Applicable documents taxonomy**	**Reference to the documents**	**Coverage of stakeholders**	**Coverage of 5G technological and functional domains**	**Coverage of lifecycle processes**
Are there mechanisms in place to inform users about potentially vulnerable end user devices, including IoT devices and of related risks?	None	None	None	None	None
Has guidance been provided to consumers and enterprises on signalling threats in legacy network environments (associated with SS7, GTP and Diameter signalling protocols) such as location tracking, interception of data, call, e-mail and SMS messages, financial fraud and theft or digital identity theft and highlighting the risk of using SMS as a multi-factor authentication mechanism?	Guideline	SECASSUR	Telecom	None	Run

TP-06-22-113-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-568-5
DOI 10.2824/700472